NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

PUTTING THE CRITICAL BACK IN CRITICAL INFRASTRUCTURE

by

Bradford C. Mason

December 2015

Thesis Advisor: Rudolph P. Darken
Second Reader: Thomas Mackin

Approved for public release; distribution is unlimited

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE			Form Approved OMB No. 0704–0188
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington, DC 20503.			
1. AGENCY USE ONLY ***(Leave blank)***	**2. REPORT DATE** December 2015	**3. REPORT TYPE AND DATES COVERED** Master's thesis	
4. TITLE AND SUBTITLE PUTTING THE CRITICAL BACK IN CRITICAL INFRASTRUCTURE			**5. FUNDING NUMBERS**
6. AUTHOR(S) Bradford C. Mason			
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000			**8. PERFORMING ORGANIZATION REPORT NUMBER**
9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A			**10. SPONSORING / MONITORING AGENCY REPORT NUMBER**
11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government. IRB protocol number NPS.2014.0020-IR-EP7-A.			
12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release; distribution is unlimited			**12b. DISTRIBUTION CODE** A

13. ABSTRACT (maximum 200 words)

In the context of national critical infrastructure security and resilience doctrine and deference to our federalist system and the sovereignty it demands, each of the sovereign states and their subdivisions have unilaterally interpreted their roles and priorities while still remaining true to the law of the land and national supremacy as demanded by the supremacy clause in Article VI of the United States Constitution. Each has independently structured, developed, and resourced its own critical infrastructure security and resilience program.

Due to this subjective and evolving nature of the critical infrastructure security and resilience mission nationally, a qualitative research method was best suited and used for the foundational nature of this work. A formative program evaluation was conducted through an anonymous online survey to capture the perceptions and views of critical infrastructure professionals across the nation. The survey included an evaluation on the perceptions and views of the business process, program maturity and implementation, as well as the current state of outcomes.

This thesis concludes with several key findings and recommendations based on the respondent survey data and analysis.

14. SUBJECT TERMS critical infrastructure, critical infrastructure protection, critical infrastructure security and resilience, homeland security, emergency management, lifeline sectors, resilience, tragedy of the commons, self-organized criticality, defense industrial base			**15. NUMBER OF PAGES** 233
			16. PRICE CODE
17. SECURITY CLASSIFICATION OF REPORT Unclassified	**18. SECURITY CLASSIFICATION OF THIS PAGE** Unclassified	**19. SECURITY CLASSIFICATION OF ABSTRACT** Unclassified	**20. LIMITATION OF ABSTRACT** UU

NSN 7540–01-280-5500 Standard Form 298 (Rev. 2–89)
Prescribed by ANSI Std. 239–18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release; distribution is unlimited

PUTTING THE CRITICAL BACK IN CRITICAL INFRASTRUCTURE

Bradford C. Mason
Assistant Deputy Director, New Jersey Office of Homeland Security and Preparedness
B.A., Rutgers University, 1992

Submitted in partial fulfillment of the requirements for the degree of

MASTER OF ARTS IN SECURITY STUDIES (HOMELAND SECURITY AND DEFENSE)

from the

NAVAL POSTGRADUATE SCHOOL
December 2015

Approved by: Rudolph P. Darken
Thesis Advisor

Thomas Mackin, California Polytechnic State University
Second Reader

Mohammed Hafez
Chair, Department of National Security Affairs

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

In the context of national critical infrastructure security and resilience doctrine and deference to our federalist system and the sovereignty it demands, each of the sovereign states and their subdivisions have unilaterally interpreted their roles and priorities while still remaining true to the law of the land and national supremacy as demanded by the supremacy clause in Article VI of the United States Constitution. Each has independently structured, developed, and resourced its own critical infrastructure security and resilience program.

Due to this subjective and evolving nature of the critical infrastructure security and resilience mission nationally, a qualitative research method was best suited and used for the foundational nature of this work. A formative program evaluation was conducted through an anonymous online survey to capture the perceptions and views of critical infrastructure professionals across the nation. The survey included an evaluation on the perceptions and views of the business process, program maturity and implementation, as well as the current state of outcomes.

This thesis concludes with several key findings and recommendations based on the respondent survey data and analysis.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ACRONYMS AND ABBREVIATIONS

ANL	Argonne National Laboratory
BZPP	Buffer Zone Protection Program
CDC	Centers for Disease Control
CIP	Critical infrastructure protection
CIPR	critical infrastructure protection and resilience
CIR	critical infrastructure resilience
CIRGP	Critical Infrastructure Resilience Grant Program
CMI	Consequences Measurement Index
COAG	Council of Australian Governments
CRS	Congressional Research Service
CSA	cyber security advisor
DHS	Department of Homeland Security
DPA	Defense Production Act of 1950
EMGP	Emergency Management Grant Program
ESF	emergency support function
FEMA	Federal Emergency Management Agency
GAO	Government Accountability Office
GHSAC	Governors' Homeland Security Advisors Council
HSGP	Homeland Security Grant Program
HSIB	Homeland Security Industrial Base
IP	Internet Protocol
IST	Infrastructure Survey Tool
LETPA	Consolidation of Law Enforcement Terrorism Prevention Activities
MPO	metropolitan planning organization
NCCIC	National Cybersecurity and Communications Integration Center
NGA	National Governors' Association
NIAC	National Infrastructure Advisory Council
NICC	National Infrastructure Coordinating Center
NIPP	National Infrastructure Protection Plan

NISAC	National Infrastructure Simulation and Assessment Center
NSDR	National Strategy for Disaster Resilience (Australian)
PMI	Protective Measures Index
PPD	presidential policy directive
PSA	Protective Security Advisor
PSGP	Port Security Grant Program
RI	resilience index
RISS	Regional Information Sharing System
RMI	Resilience Measurement Index
RRAP	Regional Resiliency Assessment Program
RSF	recovery support function
RYF	robust yet fragile
SAV	site assistance visit
SLTT	state, local, tribal and territorial
SLTTGCC	State, Local, Tribal and Territorial Government Coordinating Council
SOC	self-organized criticality
SPR	state preparedness report
SSA	sector-specific agency
THIRA	threat and hazard identification and risk assessment
TOC	tragedy of the commons
TRANSCOM	Transportation Operations Coordinating Committee
TSGP	Transit Security Grant Program
UASI	Urban Area Security Initiative
USIA	United States Industrial Alcohol

ACKNOWLEDGMENTS

I would like to thank my wife, Paula, and my sons, Bennett, Grant, and Reed, for their unwavering patience and total understanding and constant encouragement—529!

Thank you also to Charlie McKenna for making my participation in the NPS program possible and for your continued support; to Cherrie Black for her sage insight and advice; and to Brian O'Hara for his technical genius with numbers and data. Many thanks also go to Maulik Sanghavi, Eric Daleo, and Jim Cho for their keen minds and for being a sounding board for some whacky thoughts and ideas.

The core of my work, the respondent data, would not have been possible without Alisha Powell, Thomas MacLellan, and the National Governors' Association; Curt Parsons and the State, Local, Tribal, and Territorial Government Coordinating Council; as well as Critical Infrastructure Protection Alliance and Steve Davis—thank you all for your time and willingness to distribute my survey. Thank you also to each respondent who took the time out of his or her day to share candid thoughts and to complete my survey.

Certainly not least, I must thank my advisors Rudy Darken and Tom Mackin—you were both in it for the duration. Thank you.

Sincere thanks to all my classmates, as well as the instructors and staff at the Naval Postgraduate School—you have an incredible program.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

The superior man, when resting in safety, does not forget that danger may come.
When in a state of security, he does not forget the possibility of ruin.
When all is orderly, he does not forget that disorder may come.
Thus his person is not endangered, and his states and all their clans are preserved.
—Confucius (551 BC–479 BC)

A. PROBLEM STATEMENT

In accordance with the federalist system on which our government is predicated, *Presidential Policy Directive 21* and the *National Infrastructure Protection Plan* (NIPP),[1] as published by the U.S. Department of Homeland Security with stakeholder input, outlines very specific federal leads, and federal critical infrastructure protection (security and resilience) related responsibilities within the federal government that serve as federal cornerstones. However, as should be expected, these documents describe much broader, vaguer, and softer roles and responsibilities to be prescribed to state and local governments. With due deference to our federalist system and the sovereignty it demands, this lack of clarity rightfully allows each of our sovereign states and their subdivisions to unilaterally interpret their roles and priorities while still remaining true to the law of the land and federal supremacy as demanded by the supremacy clause in Article VI of the United States Constitution. Even though each generation of published national doctrine does bring more clarity to the specific roles and responsibilities of each level of government,[2] there is no common template or architecture on which any one or all of the several states' approaches to critical infrastructure protection (security and resilience) and their engagement strategies

[1] White House, *Presidential Policy Directive/PPD-21: Critical Infrastructure Security and Resilience* (Washington, DC: White House, 2013), https://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil, 11; U.S. Department of Homeland Security, *NIPP 2013: Partnering for Critical Infrastructure Security and Resilience* (Washington, DC: U.S. Department of Homeland Security, 2013), http://www.dhs.gov/publication/nipp-2013-partnering-critical-infrastructure-security-and-resilience.

[2] Pamela N. Broughton, "Measuring Preparedness: Assessing the Impact of the Homeland Security Grant Program" (master's thesis, Naval Postgraduate School, 2009), 30.

with private and public sector partners can be modeled. Therefore, as would be expected, each of the sovereign states and their subdivisions have independently structured, developed, and resourced their own programs, which has led to inconsistent critical infrastructure protection program development and implementation among the states.

Furthermore, in addition to having uneven expectations and responsibilities, most state and local jurisdictions appear to have uneven resources dedicated to the critical infrastructure protection mission.[3] This thesis explores the local adaption that has occurred[4] and the current state of the critical infrastructure community and its mission. This exploration will enhance our collective understanding as to whether the current approach and resources are adequate to meet the mandates, expectations, and assertions made on the critical infrastructure protection (security and resilience) community. Additionally, this thesis examines the current state of the "integrated network" of critical infrastructure protection partners and the "collective expertise" that former U.S. Department of Homeland Security Secretary Chertoff describes in the 2009 *National Infrastructure Protection Plan* (NIPP).[5]

The foundational nature of this work provides insight into whether our federalist system, perhaps coupled with profit motivated private critical infrastructure owners and operators, is creating an environment that allows a strategic tragedy of the commons (TOC)[6] at a national level to develop within the critical infrastructure community. This is important to recognize because if national TOC is unmitigated, it could eventually lead to the degradation,

---

[3] Curtis Parsons, and Brian Wright, *Summary of Regional Reports: Critical Infrastructure Programs 2011–2013* (Washington, DC: United States Department of Homeland Security: State, Local, Tribal, and Territorial Government Coordinating Council).

[4] Raphael Sagarin, "Natural Security for a Variable and Risk-Filled World," *Homeland Security Affairs* 6, no. 3 (September 2010): 8, https://www.hsaj.org/articles/79.

[5] U.S. Department of Homeland Security, *National Infrastructure Protection Plan: Partnering to Enhance Protection and Resiliency* (U.S. Department of Homeland Security, 2009), i.

[6] Ted G. Lewis, *Bak's Sand Pile: Strategies for a Catastrophic World* (Williams, CA: Agile Press, 2011), 16–22.

dysfunction, or collapse of our protection framework. In this case, in the context of a weak protection mission space, it is postulated that business decisions shaped by profit or fiscal efficiencies could lead to self-organized criticality (SOC)[7] within and among the established critical infrastructure sectors. In this context, SOC can be described as too much ownership of the protection mission space of an asset or process by a single entity and TOC can be described as too little ownership by any one entity.

Similar to a "catastrophic" event, where the term "catastrophic" can have a sliding definition based on the impact acuity on a defined jurisdiction, so too does "critical" have a sliding definition that shapes our understanding of what should be deemed "critical" from a national, state, or local perspective. As a nation, it is in our interests to better understand whether current expectations and understandings of the critical infrastructure community are aligned with the reality of critical infrastructure organizations nationally. This thesis establishes a ground truth of the current state of state and local critical infrastructure organizations and the national community in the United States.

B. RESEARCH QUESTIONS

It is obvious that at any level, we simply cannot afford to protect everything that may be vulnerable. Therefore, a discussion of "criticality" is essential. Question 1 asks for the status of resources available for this mission, and Question 2 asks how well our obligations are defined and how well those obligations are met. Determining how we define what is critical will allow us to "draw a line" and distinguish between essential infrastructure components and those that we may like to protect but that are less essential. It allows us to prioritize in ways we have not done before.

[7] Ibid.

(1) Primary Questions

- How is the critical infrastructure community at the state and local government level currently resourced to fulfill its critical infrastructure protection (security and resilience) mission?
- How is the federal and state, local, tribal, and territorial (SLTT) protection (security and resilience) mission space framed by the federal approach and support to this mission space?

(2) Secondary Questions

- Are the state and local critical infrastructure resources currently dedicated to the mission adequate to fulfill the defined critical infrastructure protection (security and resilience) mission?
- What recommendations and/or refinements can be made to allow state and local government the opportunity to more effectively and efficiently execute the critical infrastructure protection (security and resilience) mission?

II. LITERATURE REVIEW

This literature review is not intended to be an all-inclusive, comprehensive compilation, or exhaustive analysis of the literature associated with critical infrastructure protection, security or resilience—it cannot be. The volume of work prohibits it. Rather, it is intended to frame the landscape and contours of the existing body of associated work. It appears that most literature specific to critical infrastructure falls under one of two prevailing categories—technical literature and programmatic literature.

There are volumes of technical literature on critical infrastructure in the United States. This scientific literature tends to be scholarly and tends to center around the technical performance and operation of assets and asset subcomponents as well as technical methodologies for analysis and assessment of infrastructures. The programmatic literature generally appears in the form of public doctrine, which generally outlines national concepts, expectations, goals as well as some tools and methods. Most of this identified literature falls within three subcategories: industry associations, academic science, and government doctrine and white papers or reports. Most of the academic writing appears to be concentrated on the scientific efforts to model, harden, and identify dependencies and interdependencies within and between sectors of critical infrastructure. Much of the industry and professional association literature is focused on the current state of different sectors, emerging trends, and scientific thought centered around the modeling of critical infrastructure. Much of what is presented is of a scientific nature, and seeks to understand the mathematics behind the models.

Though there is a broad set of public doctrine and associated expectations and mandates for critical infrastructure professionals across the country, there appears to be very limited non-scientific scholarly programmatic literature on the policy side of critical infrastructure protection (security and resilience). An exploration of the Homeland Security Digital Library, the Naval Postgraduate School's Dudley Knox Library, the Library of Congress's Congressional Research

Service (CRS), and the United States Government Accountability Office (GAO) has identified a finite set of federal government and national doctrine and documents such as the *National Infrastructure Protection Plan* (NIPP), [8] *Homeland Security Presidential Directive 7*,[9] numerous CRS reports and GAO reports for analysis. Cornerstone public doctrine that outlines contemporary concepts, expectations, assertions, and mandates, includes sources such as the Homeland Security Act of 2002 (Public Law 107-296), President Bush's *National Strategy for the Physical Protection of Critical Infrastructures and Key Assets*[10] and President Obama's *Presidential Policy Directive / PPD-21: Critical Infrastructure Security and Resilience*.[11]

In his 2003 national strategy, President Bush first set out to define the strategic objectives and desired end state of our then new collective national mission of physical protection. [12] Framing our current thinking on critical infrastructure security and resilience, President Obama issued PPD-21 on February 12, 2013. PPD-21 describes the unique role of owners and operators of critical infrastructure[13] and describes the national policy and endeavor of critical infrastructure security and resilience as a "shared responsibility amongst Federal, state, local, tribal and territorial (SLTT) entities and public and private owners and operators of critical infrastructure." [14] The directive further re-defines the 16 critical infrastructure sectors,[15] the roles and responsibilities of federal partners

[8] U.S. Department of Homeland Security, *NIPP 2013*.

[9] U.S. Department of Homeland Security, *Homeland Security Presidential Directive 7: Critical Infrastructure Identification, Prioritization, and Protection* (Washington, DC: U.S. Department of Homeland Security, 2003), http://www.dhs.gov/homeland-security-presidential-directive-7.

[10] White House, *The National Strategy for The Physical Protection of Critical Infrastructures and Key Assets* (Washington, DC: White House, 2003).

[11] White House, *Presidential Policy Directive/PPD-21*.

[12] White House, *The National Strategy for The Physical Protection*, vii.

[13] White House, *Presidential Policy Directive/PPD-21*, 2.

[14] Ibid.

[15] Ibid., 15–16.

and federal sector-specific agencies (SSA),[16] as well as outlines the "three strategic imperatives" that drive the federal approach to critical infrastructure security and resilience.[17]

The president is clear that effective implementation of his directive will require a "national unity of effort" that must include the federal sector-specific agencies and other federal departments and agencies, as well as a strong collaboration and partnership of the federal community with critical infrastructure owners and operators and SLTT entities.[18] The collaboration and partnership imperative, and the president's call to action of critical infrastructure owners and operators as well as SLTT entities are also clear. In the context of state sovereignty and national supremacy, the president explicitly identifies the need for federal partners to collaborate and partner with critical infrastructure owners and operators and SLTT entities throughout his directive. With "SLTT entities" referred to at least 12 times in PPD-21, it becomes important to gain an insight or to better understand what these SLTT entities are, the imperatives that drive their approach, and how the entities are staffed and resourced. This collective insight or understanding is an important baseline to establish to further define the appropriate and reasonable roles of all critical infrastructure security and resilience partners and to determine whether these partners are similarly or proportionately postured and equipped to achieve the necessary national unity of effort.

In 2009, the National Infrastructure Advisory Council (NIAC) found the need for clarified roles and responsibilities of critical infrastructure partners.[19] Established by President Bush's Executive Order 13231, the NIAC was created to provide the president and federal departments and agencies non-federal

---

[16] Ibid., 4–8, 15–16.

[17] Ibid., 3–4, 9–11.

[18] Ibid., 4.

[19] National Infrastructure Advisory Council, *Critical Infrastructure Resilience: Final Report and Recommendations* (Washington, DC: National Infrastructure Advisory Council, 2009), 19, http://www.dhs.gov/xlibrary/assets/niac/niac_critical_infrastructure_resilience.pdf.

executive level advise on critical infrastructure sectors through the secretary of the Department of Homeland Security.[20] [21] The NIAC has met regularly since its creation on October 16, 2001. In addition, since 2004, it has conducted a wide range of critical infrastructure related studies and has published associated study reports and recommendations.

The council's final report and recommendations on critical infrastructure resilience was published on September 8, 2009. This report was conducted in three phases that centered on developing a working definition of resilience, cataloging the current government and business efforts of the day to promoted resilience, and the development of actionable recommendations that were associated with the six findings outlined in the report.[22] Of note, the word "government" is used throughout the report with no distinction of jurisdiction or level of government. This could be purposely reflective of the inclusive nature of NIAC's work, indicative of the collaborative nature of the public sector critical infrastructure enterprise, or perhaps reinforce the implicit need for further definition and role clarity within the enterprise. By design, the NIAC's advise to the president and federal community represents the perspective of private sector executives; therefore, the use of the broad word "government" could also be a simple matter of convenience not unlike the wide use of "public sector" or "private sector."

A series of regional reports and an associated summary document published by the U.S. Department of Homeland Security State, Local, Tribal and Territorial Government Coordinating Council (SLTTGCC),[23] which begins to explore SLTT critical infrastructure security and resilience organizations and programs, appears to be the most recent programmatic literature available as

[20] Exec. Order No. 13231 (2001), http://www.dhs.gov/xlibrary/assets/executive-order-13231-dated-2001-10-16-initial.pdf.

[21] National Infrastructure Advisory Council, *Critical Infrastructure Resilience*, 4.

[22] Ibid., 7, 16–27.

[23] Parsons, and Wright, *Summary of Regional Report*, 1–22.

secondary data to shape and inform the work of this thesis and our national thinking.

As legally established in 2007 and further defined by the 2009 *National Infrastructure Protection Plan* (NIPP),[24] the SLTTGCC is comprised of national critical infrastructure protection leaders and partners from across the United States. In an effort to better understand its own community and constituents, the SLTTGCC commissioned a review and analysis of state and local partners by associated federal regions and published 10 regional reports and a summary roll-up document that outlines existing and emerging organizational and programmatic themes.[25] This SLTTGCC study was based on 284 direct interviews of critical infrastructure partners and practitioners that focused on SLTT program structure, activities, and needs across all 10 federal regions.[26] It concluded, in part, that despite being focused on the same common elements of critical infrastructure security and resilience as outlined in the NIPP,[27] no two programs across the nation were organized, staffed, and resourced similarly.[28] Furthermore, the final report summarized 39 findings that included general themes by federal region, critical infrastructure program fundamentals, best practices, and top needs of the SLTT critical infrastructure community.[29]

Driven in part by the resilience requirements of PPD-21[30] and similar in nature to the 2009 NIAC critical infrastructure resilience report, another facet of

---

[24] U.S. Department of Homeland Security, *National Infrastructure Protection Plan*, 2.

[25] Parsons, and Wright, *Summary of Regional Report*, 1–22.

[26] Ibid., 2–4.

[27] U.S. Department of Homeland Security, *NIPP 2013*, 15.

[28] Parsons, and Wright, *Summary of Regional Report*, 4.

[29] Ibid., 2–4.

[30] F. D. Petit et al., *Resilience Measurement Index: An Indicator of Critical Infrastructure Resilience* (Argonne, IL: Argonne National Laboratory: Decision and Information Sciences Division, 2013), ix, http://www.ipd.anl.gov/anlpubs/2013/07/76797.pdf; Penny Pritzker, "Community Resilience Planning Guide for Buildings and Infrastructure Systems: Volume II—Draft for Public Comment" (Washington, DC: National Institute of Standards and Technology, 2015), 230, http://www.nist.gov/el/building_materials/resilience/upload/NIST_Guide_Volume_2_042515_For-Web-2.pdf.

related literature that appears to be an emerging subcategory of both the technical and programmatic critical infrastructure literature is focused on resilience. This emerging subcategory of resilience literature appears to center around how resilience is or can be defined, measured, and/or achieved. Much of this emerging subcategory of literature is blended government reports or papers that contain or catalog both technical and programmatic issues of resilience. Amplifying the definition of *resilience* provided in PPD-21,[31] this literature tends to describe the common core resilience elements in terms of absorption, adaptation, and recovery, as well as additional companion, derivative, or variant elements of each. [32] Examples of these blended technical and program documents include the comprehensive National Academy of Sciences report *Disaster Resilience: A National Imperative.*[33] Open meetings and field visits to collect data in the Gulf of Mexico coast states of Louisiana and Mississippi, as well as in Iowa and southern California, serve as the backdrop to the study.[34] The study report outlines resilience in terms of understanding and managing risk, resilience leadership and investments, metrics and measurement of progress, local engagement, and capacity, policy, and the way forward.[35]

Since August 2010, the U.S. Department of Energy's Argonne National Laboratory (ANL) has published three reports on the specific topic of resilience. It appears that the first and third reports of this series were primarily written to

---

[31] White House, *Presidential Policy Directive/PPD-21*, 17.

[32] U.S. Department of Homeland Security, *NIPP 2013*, 7; L. Carlson et al., *Resilience: Theory and Applications* (Argonne, IL: Argonne National Laboratory: Decision and Information Sciences Division, 2012), vii, 21–22, http://www.ipd.anl.gov/anlpubs/2012/02/72218.pdf.

[33] Committee on Increasing National Resilience to Hazards and Disasters, *Disaster Resilience: A National Imperative* (Washington, DC: National Academies Press, 2012), http://resilience.abag.ca.gov/wp-content/documents/resilience/toolkit/Disaster%20Resilience_A%20National%20Imperative.pdf.

[34] Ibid., viii.

[35] Committee on Increasing National Resilience to Hazards and Disasters, *Disaster Resilience*, xv–xvi, 1–9.

outline the development of a resilience measurement index (RMI).[36] These publications outlined the thinking, function and utilization of the RMI to support the DHS Office of Infrastructure Protection's Infrastructure Survey Tool (IST) and protective security advisors (PSA) conducting site assistance visits (SAV).[37] The first report was more foundational in nature and conceptually outlined the RMI pre-cursor, the proposed ANL resilience index (RI).[38] The third report outlined the evolved and matured thinking of the RMI and how the RMI compliments the two ANL companion indices: the Protective Measures Index (PMI) and the Consequences Measurement Index (CMI).[39]

The second in the ANL resilience report series, *Resiliency: Theory and Applications* is less technical in nature and provides more of a policy narrative on the evolving contours of the RMI and of measuring and evaluating community and regional resilience.[40] The report goes on to describe critical infrastructure as one community or regional subsystem among several subsystems important to achieving overall resilience. In addition to the critical infrastructure subsystem, ANL suggests that the other threads in the community and regional resilience fabric include the economic, civil society, supply chain/dependencies and governance/institutional subsystems.[41] Released during the writing of this thesis, the U.S. Department of Commerce National Institute of Standards and Technology (NIST) recently published a rich and blended draft volume set titled *Community Resilience Planning Guide for Buildings and Infrastructure*

[36] Petit et al., *Resilience Measurement Index*; R. E. Fisher et al., *Constructing a Resilience Index for the Enhanced Critical Infrastructure Protection Program* (Argonne, IL: Argonne National Laboratory: Decision and Information Sciences Division, August 2010), http://www.ipd.anl.gov/anlpubs/2010/09/67823.pdf.

[37] Fisher et al., *Constructing a Resilience Index*, ix–1, 14–16, 19–22.

[38] Ibid., 1–7, 21–27.

[39] Petit et al., *Resilience Measurement Index*, x–2, 4–5, 15–16, 23–26, 29.

[40] Carlson et al., *Resilience: Theory and Applications*.

[41] Ibid., 19–29.

Systems.[42] Rather than simply outlining the issues, justifications, or aspirational goals to achieve community resilience—the "whats" and "whys" of resilience—the draft NIST volumes attempt to put forth a blueprint to assist communities on "how" to operationally achieve it.

From the practical to the abstract, several books have also been recently published on the different aspects of resilience. For instance, Dane Egli published his book *Beyond the Storms* during the writing of this thesis. Egli's book is a mostly practical catalog that amplifies the numerous evolving issues and themes associated with the contemporary discussion on achieving resilience. Additionally, he outlines the conceptual roots of resiliency and explains that the deeper the resiliency roots of infrastructure, the more likely infrastructure is too stand-up to all-hazard stressors.[43] Half of Egli's volume is a compilation of 13 case studies that he uses to illustrate his recommendations and priorities necessary to achieve resilience. Another source published in 2012, is Andrew Zolli's book *Resilience*, which is more of an abstract writing about resilience and the dynamics of the larger human experience.[44] Beyond the resilience elements of absorption, adaptation, and recovery, Zolli explores the individual and collective characteristics of people and the systems on which we are dependent. Throughout the book, Zolli illustrates his ideas with stories and anecdotes along with historical and contemporary real-world examples about the notion of robust yet fragile (RYF), scale, swarms clusters, cooperation, cognitive diversity, and leadership.[45]

---

[42] Pritzker, "Community Resilience Planning Guide, Vol II;" Penny Pritzker, "Community Resilience Planning Guide for Buildings and Infrastructure Systems: Volume I—Draft for Public Comment" (Washington, DC: National Institute of Standards and Technology, 2015), http://www.nist.gov/el/building_materials/resilience/upload/NIST_Guide_Volume_1_042515_For-Web-2.pdf.

[43] Dane S. Egli, *Beyond the Storms: Strengthening Homeland Security and Disaster Management to Achieve Resilience*, 1st ed. (Armonk, NY: M. E. Sharpe, Inc., 2014), 30.

[44] Andrew Zolli, *Resilience: Why Things Bounce Back*, 1st ed. (New York: Free Press, 2012).

[45] Ibid., 27–28, 40, 49, 61, 65, 68–71, 93, 156–159, 210, 239.

The Commonwealth of Australia has also published noteworthy government doctrine and reports. The United States and Australia both maintain a federalist form of government. Comprised of 10 states and territories, the commonwealth is roughly equivalent (yet slightly smaller) in geographic size to the contiguous 48 states of the United States.[46] It has a current approximate population that is roughly equal to the combined population of the states of New York and Kansas (approximately 22.4 million people)[47]; the Australian population is approximately 22.6 million people.[48] Given this, neither the Australian population density nor the concentration of infrastructure is close to that of the United States. However, the similarities in geographic size, the federalist form of government, and the critical infrastructure practices employed by the Australian government makes for an interesting comparative example.

It is clear in current Australian doctrine that national security is national security with no distinction to be made about the Australian homeland—homeland security in Australia is inherently national security (unlike in the U.S. where there is some enterprise overlap and some separation). The broader and inter-connected context of the national security environment in Australia includes both traditional and "non-traditional threats such as organized crime, natural disasters and pandemics."[49] In 2009 and similar to what President Obama outlined and directed in PPD-21, Australia formally shifted the thinking of its Critical Infrastructure *Protection* Program to Critical Infrastructure *Resilience*—a subtle yet profound shift in focus. The commonwealth anchored this shift in thinking with the publication of the *Critical Infrastructure Resilience Strategy* and

[46] Central Intelligence Agency, "Australia," *The World Factbook*, https://www.cia.gov/library/publications/the-world-factbook/geos/as.html.

[47] U.S. Census Bureau, "State and County Quick Facts" [New York, Kansas], http://quickfacts.census.gov/qfd/states/36000.html.

[48] Ibid.

[49] Commonwealth of Australia, *Critical Infrastructure Resilience Strategy*, 2010, http://www.ag.gov.au/Nationalsecurityandcounterterrorism/Pages/CriticalInfrastructureResilience.aspx, 6.

the *Strategy Supplement: An Overview of Activities to Deliver the Strategy*.[50] Built on its traditional critical infrastructure protection efforts, the Australian critical infrastructure resilience (CIR) strategy is a whole-of-nation, all-hazards approach, which at the commonwealth level of government, is directly managed by the Attorney-General's Department. The new CIR program maintains the "protection" aspect of critical infrastructure as one element of the overall resiliency mission. Similar to the United States, but perhaps a bit tighter in scope, the Australian government recognizes critical infrastructure as that which underpins all other essential services; these underpinnings include power, water, health, communications systems, and banking.[51] In the United States, these named sectors are equal in importance, and they are thought to be the lifeline[52] critical infrastructure sectors of the now 16 critical infrastructure sectors outlined in the 2013 *National Infrastructure Protection Plan* (NIPP).[53] As is the case in the United States' security and resilience mission, engagement with the private sector owners and operators is the centerpiece to the current Australian CIR strategy.[54]

[50] Commonwealth of Australia, *Critical Infrastructure Resilience Strategy Supplement: An Overview of Activities to Deliver the Strategy*, 2010, http://www.emergency.qld.gov.au/publications/pdf/Critical_Infrastructure_Resilience_Strategy_Supplement.pdf.

[51] Ibid., 3.

[52] Constance H. Lau, and Beverly Scott, "Strengthening Regional Resilience through National, Regional and Sector Partnerships—DRAFT Report and Recommendations" (Washington, DC: National Infrastructure Advisory Council, 2013), http://www.dhs.gov/sites/default/files/publications/niac-rrwg-report-final-review-draft-for-qbm.pdf; Brandon J. Hardenbrook, "The Need for a Policy Framework to Develop Disaster Resilient Regions," *Journal of Homeland Security and Emergency Management* 2, no. 3 (2005), doi:10.2202/1547-7355.1133.

[53] U.S. Department of Homeland Security, *NIPP 2013*, 11.

[54] Commonwealth of Australia, *Critical Infrastructure Resilience Strategy*, 12–13.

III. METHODOLOGY

Due to the subjective and evolving nature of the critical infrastructure security and resilience mission nationally, a qualitative research method was best suited and used for the foundational nature of this work. A formative program evaluation was conducted through a national online anonymous survey to capture the views of critical infrastructure professionals. The survey included an evaluation on the perceptions of the business process, maturity and implementation, and current state of outcomes.

This formative research centered on an online national survey of critical infrastructure protection professionals conducted through the approved Naval Postgraduate School's enterprise survey tool, *Lime Survey*. The survey was completely anonymous and voluntary in nature, and no personally identifiable information, Internet Protocol (IP) address, or other electronic signature was captured during this survey.

The survey was open for respondent participation from Tuesday, June 17, 2014 to Thursday, July 31, 2014—approximately seven full weeks. During the open participation period, there were a total of 135 hits on the internet survey link recorded. The system recognized 15 people that navigated away from the survey link before starting the survey. A total of 120 respondents fully or partially participated. Of the 120 total respondents, 84 people completed the entire survey, and 36 people partially completed the survey.

The online survey consisted of 48 questions structured into four sections, which included basic information about the respondent's background and affiliation (role in the critical infrastructure enterprise), perceptions on strategic business process maturity and implementation, views on operational business process maturity, and implementation as well as perceptions on the current state of the critical infrastructure enterprise and current outcomes.

Participants were asked to rate their perceptions by utilizing a Likert[55] scale of strongly disagree, somewhat disagree, disagree, agree, somewhat agree, or strongly agree. The *Lime Survey* tool captured the number of respondents for each question and the rating provided. This data was then utilized to calculate averages and composite percentages.

A. AVERAGE RESPONDENT SCORE

To evaluate the response averages; each Likert[56] rating scale was converted to a numeric value. For those perception-based questions that included an "I don't know" response option, the "I don't know" answer was assigned a "99" value as a numeric flag and dropped from the average equation. No further evaluation or action was taken with these "99" values. Numeric values were assigned as follows:

Strongly disagree	= 1
Somewhat disagree	= 2
Disagree	= 3
Agree	= 4
Somewhat agree	= 5
Strongly agree	= 6
I don't know	= 99
Never	= 1
Almost never	= 2
Infrequently	= 3
Occasionally	= 4
Frequently	= 5

[55] John M. Linacre, "Investigating Rating Scale Category Utility," *Journal of Outcome Measurement: Dedicated to Health, Education and Social Science* 3, no. 2 (1999): 104–106; Janice Rattray, and Martyn C Jones, "Issues in Clinical Nursing: Essential Elements of Questionnaire Design and Development," *Journal of Clinical Nursing* 16 (2005): 235–236, doi:10.1111/j.1365-2702.2006.01573.x.

[56] Linacre, "Investigating Rating Scale Category Utility," 104–106; Rattray, and Jones, "Issues in Clinical Nursing," 235–236.

Very frequently	= 6
I don't know	= 99

For Question 8, where respondents were asked to choose one answer that best described their jurisdiction, the following nominal numeric values were assigned:

Rural	= 1
Rural-suburban	= 2
Suburban	= 3
Suburban-urban	= 4
Urban	= 5

The average numeric response value was calculated by summing all of the assigned 1–6 (or 1–5) numeric values for each question and dividing that sum by the total number of respondents (N) for each question.

$$\text{Average respondent score} = \frac{\text{sum of assigned numeric values}}{\text{total number of responses (N)}}$$

This provides an average respondent response score that serves as a benchmark of collective respondent sentiment for each perception-based question. For the Likert[57] scale-based questions, an average respondent score between 1 and 3 is an expression of disagreement. An average respondent score between 4 and 6 is an expression of agreement. For the nominal numeric values assigned in Question 8, the average respondent score is not an expression of respondent sentiment but is objectively reflective of the average type of jurisdiction respondents indicated.

B. COMPOSITE PERCENTAGES

The Microsoft Excel calculation and graphing tool was utilized to determine and depict composite percentages for each of the perception-based questions presented. In addition, graphs were generated to present the sentiment of those within each response option of each question. Each graph

[57] Ibid.

generated by the Microsoft Excel graphing tool provides a view of the proportional composition of respondents.

C. ANALYSIS

Results were examined and analyzed based on respondents' answers to each question, cross-analyzed by some of the background and affiliation data that was captured. This allowed for additional context, more insightful response analysis and the identification of trends or anomalies. A Microsoft Excel analytical tool was built and utilized for this purpose.

IV. CRITICAL INFRASTRUCTURE SURVEY

This section will present the survey response data analysis for each block of the online survey. Where specific questions are cited, the average respondent score (Average) and the total number of respondents to the question (N) are provided (i.e., Question xx: Average y.yy, N=zz).

A. POTENTIAL BIAS

During the approximate seven full weeks that the survey was open for respondent participation to solicit anonymous online participation in the survey, the survey recruitment script with an embedded survey hyperlink was distributed via three primary channels. The survey recruitment was distributed twice through the U.S. Department of Homeland Security Infrastructure Protection State, Local, Tribal and Territorial Government Coordinating Council (SLTTGCC), twice through the national Urban Area Security Initiative (UASI) conference email distribution list, and once by the National Governors Association (NGA) Governors' Homeland Security Advisors Council (GHSAC). These distribution channels could potentially weigh the opinion data of respondents from urban jurisdictions, state level professionals or those individuals with a vested interest in expanding their professional role or organization.

B. SURVEY SECTION: BACKGROUND AND AFFILIATION

A series of seven background and affiliation questions were asked of respondents. The responses from these questions were cross-analyzed against the perceptual responses for additional context and more insightful response analysis. Question 1 was the only mandatory question in the survey conducted. All respondents had to provide informed consent (by selecting "I consent to participate in this study") to start the survey. If a respondent navigated away from the online survey hyperlink or selected "I do not consent to participate in this study," the survey session ended. Figure 1 indicates that 91 respondents provided consent to participate in this study.

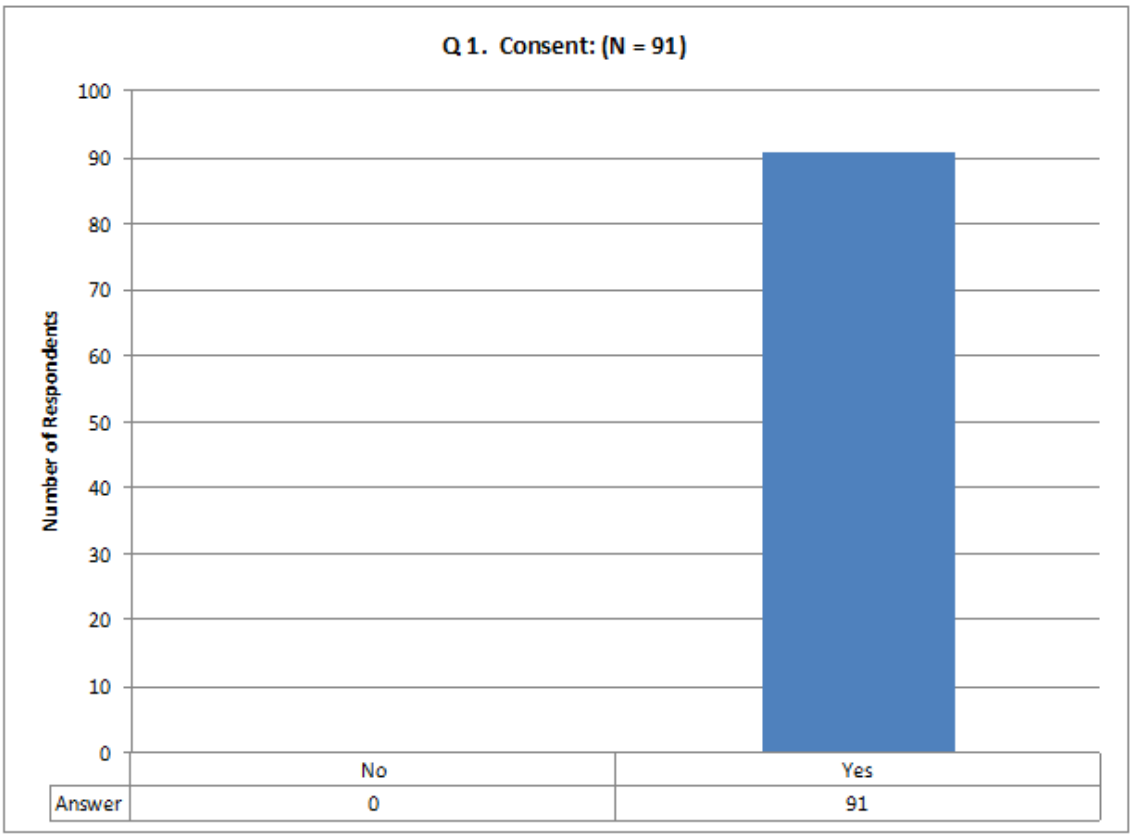


Figure 1. Consent to participate in this study.

In Question 2 (N=90), respondents were asked to self-identify as either a critical infrastructure protection (CIP) practitioner within their jurisdiction or as a member of a partner organization to their jurisdiction's CIP practitioners. This question was asked to better understand a respondent's perspective with which she or he was completing the study. As indicated in Figure 2, 61 respondents (67.77 percent) self-identified as a CIP practitioner, 29 respondents (32.22 percent) self-identified as a member of a partner organization, and one respondent did not self-identify.

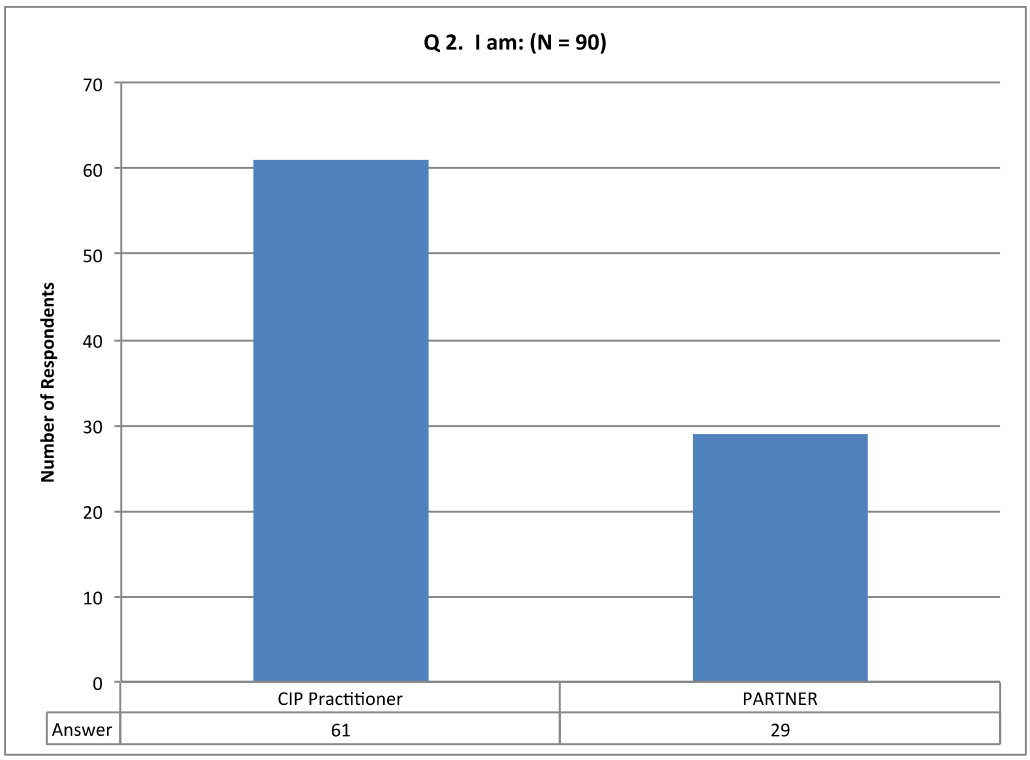


Figure 2. Self-identification as a CIP practitioner or partner.

Question 3 (N=90) asked respondents to provide their state/territory of jurisdiction or the state/territory within which their primary jurisdiction exists. As shown in Figure 3, responses were then aligned to the 10 FEMA regions for analytical purposes to understand what, if an, geographic distinctions exist.

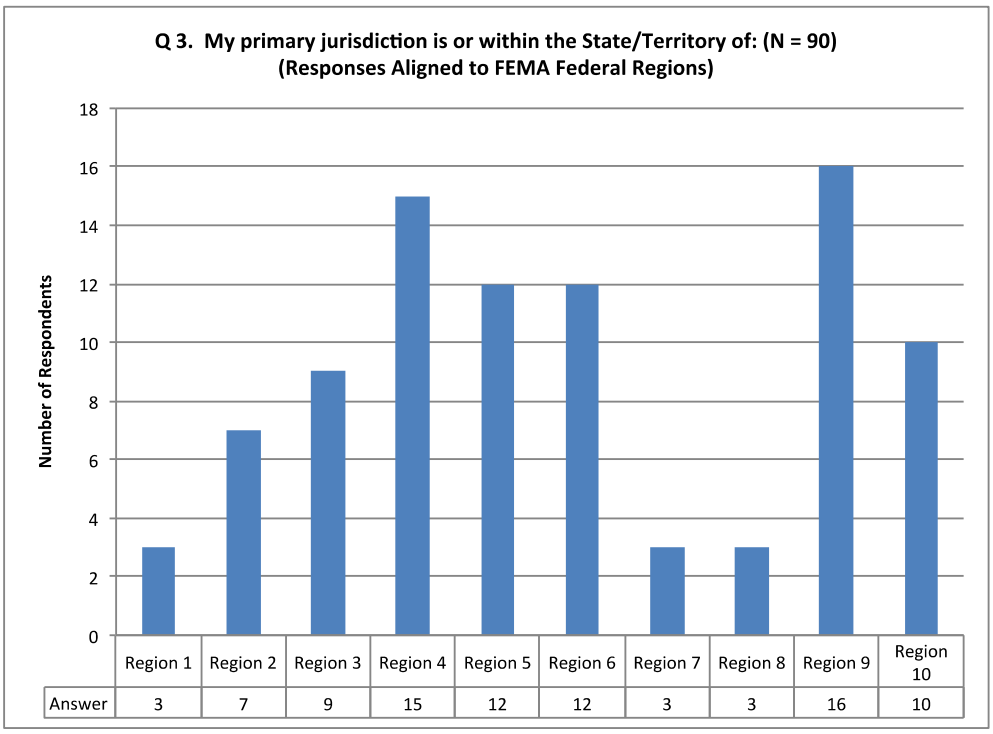


Figure 3. State/territory alignment to the 10 federal FEMA regions.

Question 4 (N=91) was asked to determine the type of organization with which respondents identified by selecting the choice that best described their organization. The survey provided 11 different options. An "other" option was also provided within which a narrative response could be provided if a respondent did not consider the provided choices appropriate or accurate. This response data is important to understand respondents' perspective when cross-analyzed against perceptual response data. As indicated in Figure 4, the top five best organizational descriptions included 32 respondents (35.16 percent) who selected "emergency management," 16 respondents (17.58 percent) selected "law enforcement," 15 respondents (16.48 percent) selected "homeland security," 11 respondents (12.08 percent) selected "other," and eight respondents (8.79 percent) critical infrastructure protection (CIP)."

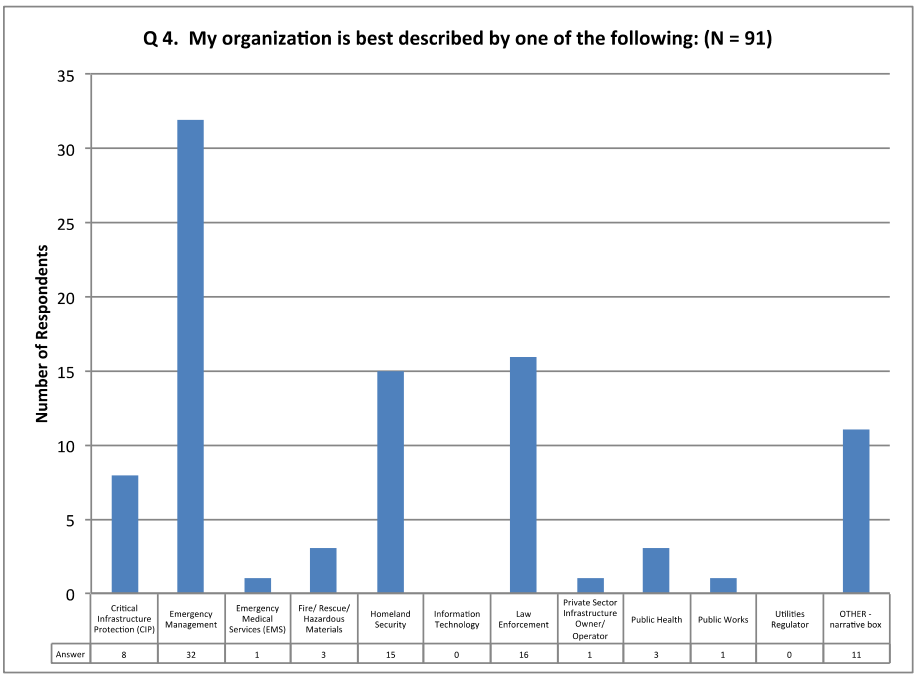


Figure 4. Best description of respondents' organization.

Question 5 (N=91) asked respondents to determine the organizational role with which they identified by selecting the choice that best described their title or position. The survey provided seven different options, and an "other" option was also provided within which a narrative response could be provided if a respondent did not consider the provided choices appropriate or accurate. This response data is important to understand respondents' organizational perspective and provide additional context when cross-analyzed against perceptual response data. As indicated in Figure 5, the top five best descriptions of respondents' roles within their organization included 29 respondents (31.86 percent) who selected "program manager," 20 respondents (21.97 percent) selected "other," 15 respondents (16.48 percent) selected "director/deputy director," 13 respondents (14.28 percent) selected "manager/bureau chief," and nine respondents (9.89 percent) selected "supervisor/ team leader."

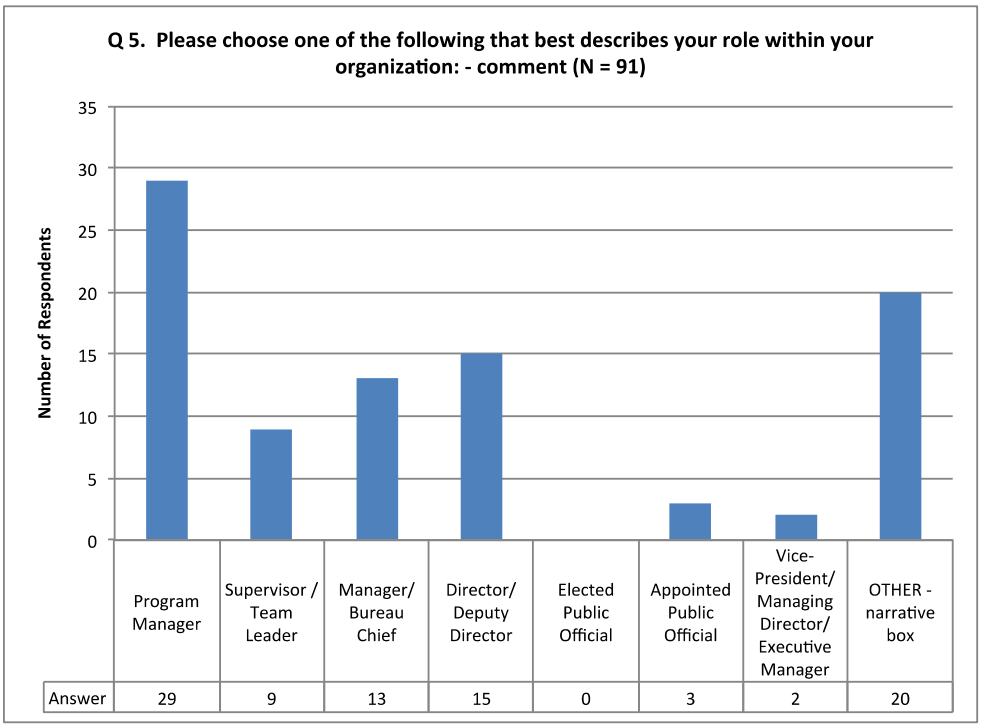


Figure 5. Best description of a respondents' role within their organization.

Question 6 (N=90) was asked to determine respondents' years of experience as a CIP practitioner or member of a partner organization. Experience level is an important analytical element to better how perceptions may change with a respondents' level of experience. As indicated in Figure 6, most respondents (70.00 percent) indicated between one and 10 years of experience as a CIP practitioner or CIP partner, 32 respondents (35.55 percent) selecting "1–5 years" of experience, 31 respondents (34.44 percent) selecting "6–10 years" of experience, and 16 respondents (17.77 percent) selecting 11–15 years of experience. The average experience of all respondents was 9.07 years.

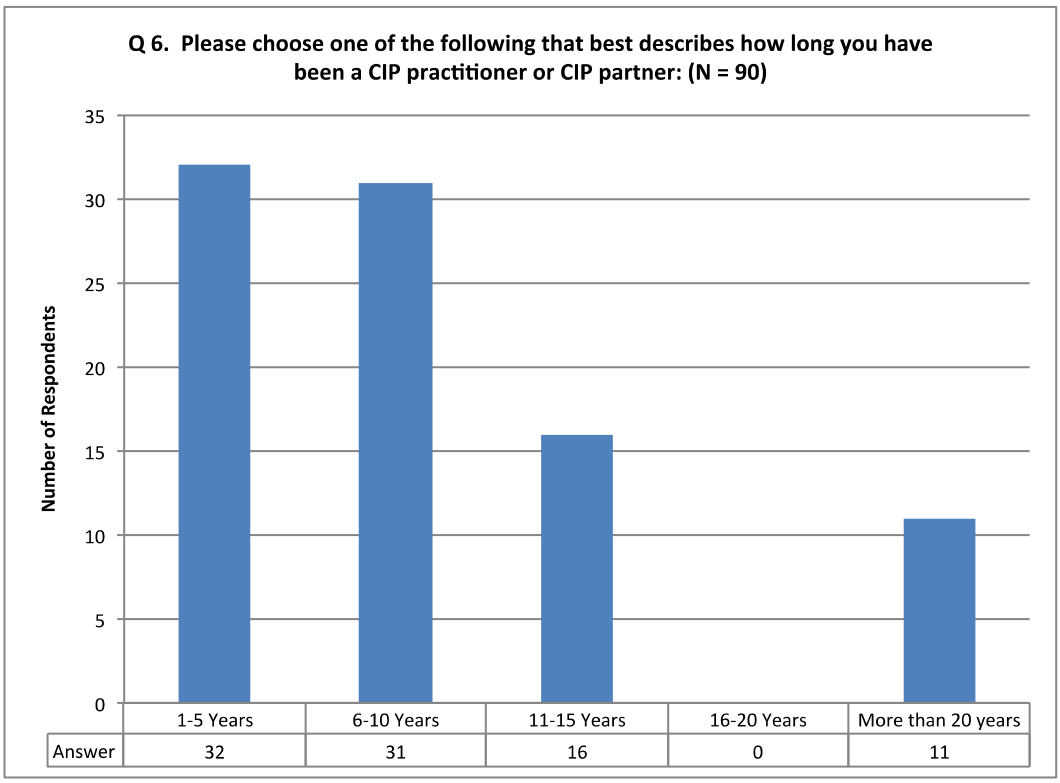


Figure 6. Years of experience as a CIP practitioner or CIP partner.

Question 7 (N=91) was asked to establish the respondents' level of government by selecting the choice that best described their jurisdiction. The survey provided six different options. An "other" option was also provided within which a narrative response could be provided if a respondent did not consider the provided choices reflective of their jurisdiction. This response data is important to understand respondents' jurisdictional perspective and provide additional context when cross-analyzed against perceptual response data. As indicated in Figure 7, the top three best descriptions of respondents' jurisdictions included 30 respondents (32.96 percent) who selected "state," 27 respondents (29.67 percent) selected "county/parish," and 22 respondents (24.17 percent) selected "city/town/village/municipal."

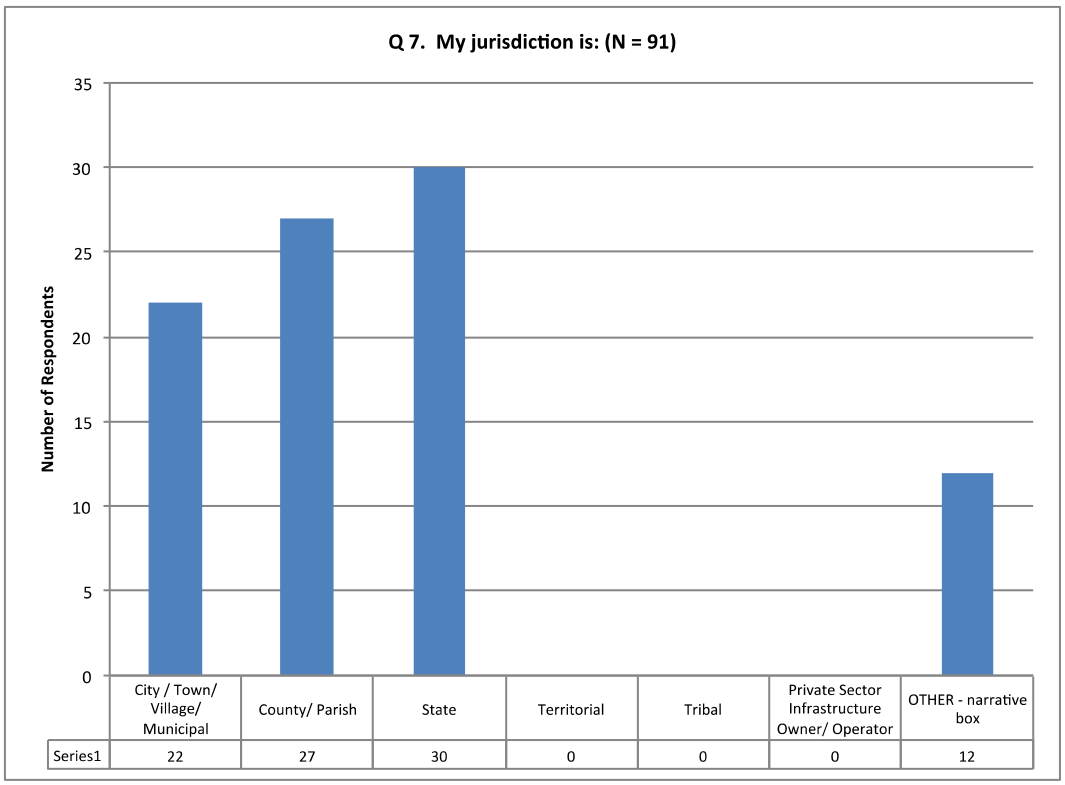


Figure 7. Respondents' jurisdiction.

Question 8 (N=87) asked respondents to qualify their jurisdiction as rural, rural-suburban, suburban, suburban-urban, or urban. This response data is important to further understand respondents' jurisdictional perspective and provide additional context when cross-analyzed against perceptual response data. Based on respondent data, Figure 8 shows that most respondents indicated that their jurisdiction was primarily suburban to suburban-urban (Question 8: Average 3.63, N=87).

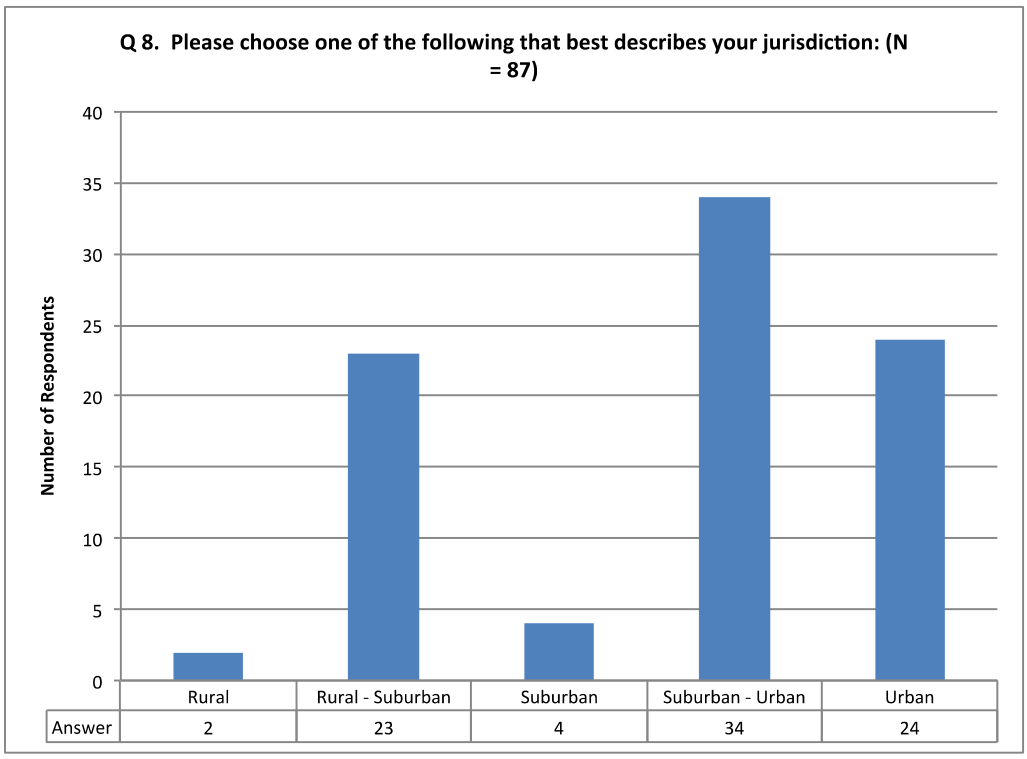


Figure 8. Respondents' jurisdiction qualified rural to urban.

C. SURVEY SECTION: PERCEPTIONS AND VIEWS OF STRATEGIC AND TACTICAL BUSINESS PROCESS

The next block of questions centered on the respondents' general perceptions and views of the strategic and tactical aspects of the critical infrastructure protection (security and resilience) enterprise. Many respondents indicated that their jurisdictions have invested their own operational funds to support staffing of their critical infrastructure protection program (37.5 percent of salary is supported by operational budgets, see Figure 9). As further indicated in Figure 9, it also appears that the financial investments in CIP staff are significantly dependent on federal grant funds (55.8 percent of salary is supported by federal financial grants, see Figure 9). Respondents indicated the use of federal financial grants to support CIP staff salaries as follows: the FEMA Homeland Security Grant Program (HSGP) is 19.5 percent of financial support, Urban Area Security Initiative (UASI) is 17.8 percent of financial support, and the FEMA Emergency Management Performance Grant (EMPG) is 11.8 percent of

the financial support of CIP staff salaries (see Figure 10). Though respondents indicated the use of other funding sources, such as private sector financial support, state grants and federal grant programs, including the Port Security Grant Program (PSGP), the Transit Security Grant Program (TSGP), and Centers for Disease Control (CDC) funding to support their CIP program salaries, the three most common types of federal grant funds invested were the HSGP, UASI and EMPG. Of note, the utilization percentages of the funding sources indicated (Figures 9–11) do not change significantly when filtered by 80 percent plus utilization of a single funding source indicating a dependence on these federal funding mechanisms.

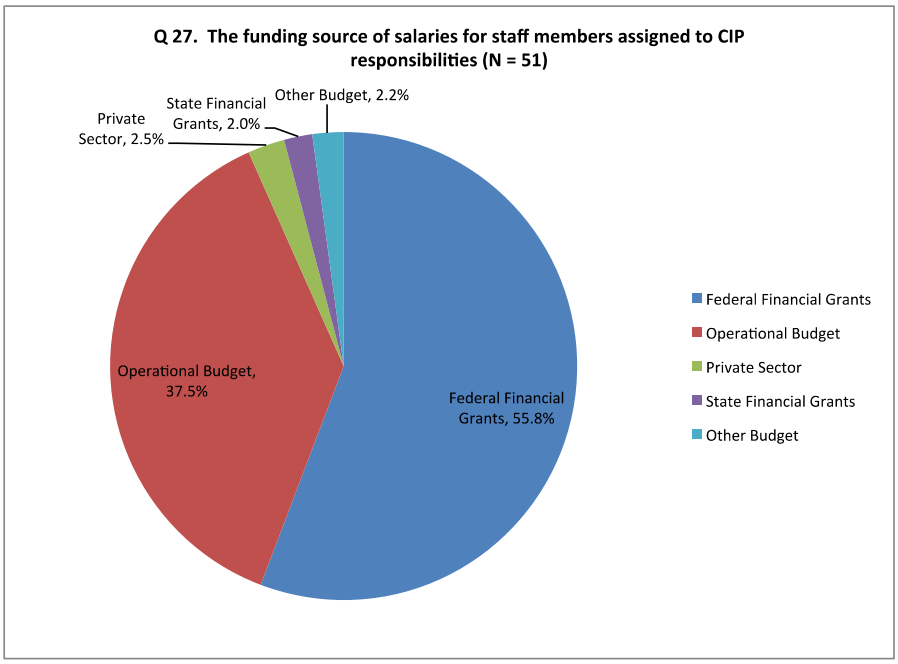


Figure 9. Funding source of CIP staff salaries.

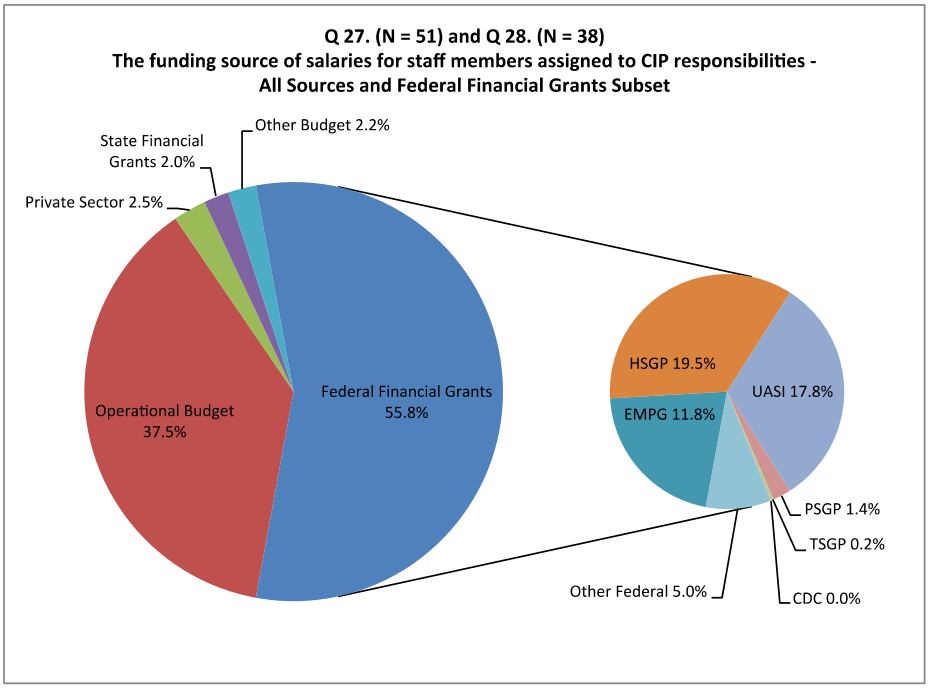


Figure 10. Funding source of CIP staff salaries with federal subset.

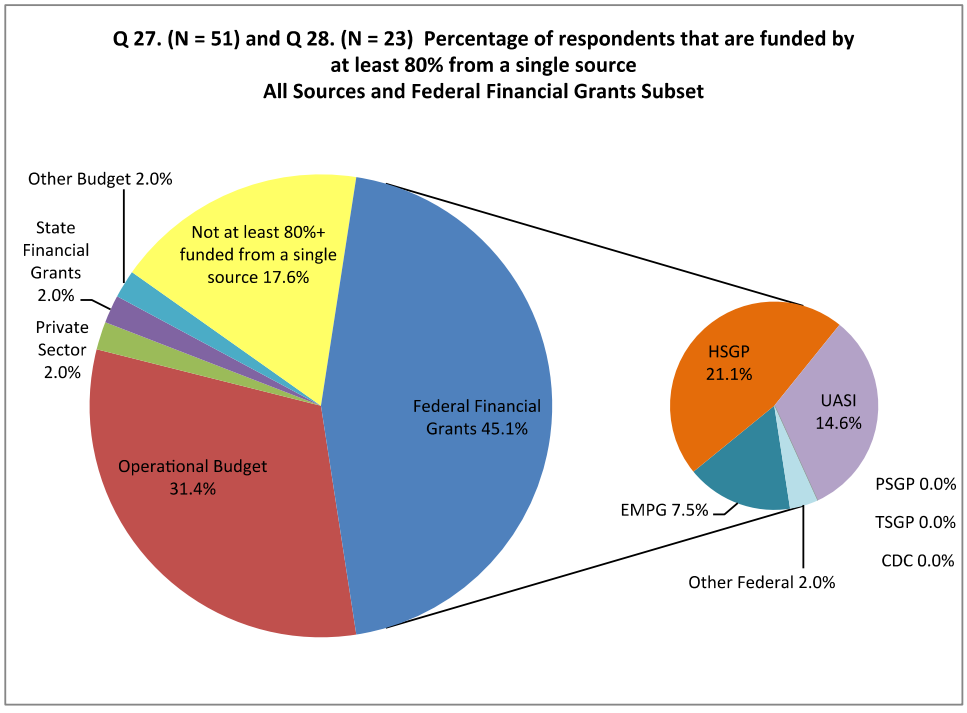


Figure 11. Funding source of CIP staff salaries with federal subset of at least 80 percent of funding coming from a single source.

The utilization of federal grant funds increases when cross-analyzed against CIP staff members where staff members are not fully dedicated to CIP program responsibilities. Figure 12 indicates a 65.6 percent utilization of federal financial grants in this instance. The high use of federal grant funds to support staff members not fully dedicated to CIP responsibilities may further indicate both a critical dependence on these federal funds and inherent programmatic vulnerability.

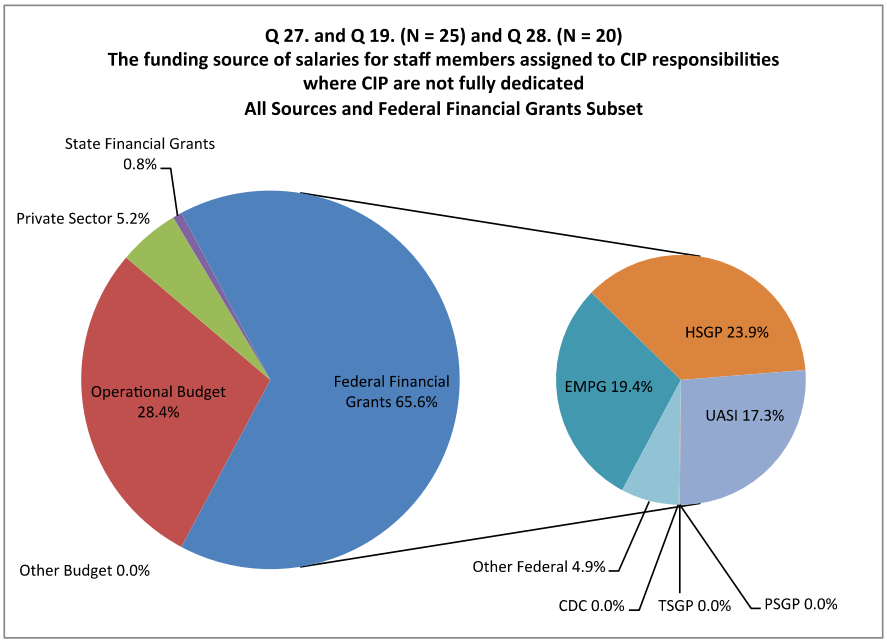


Figure 12. Funding source of CIP staff (collateral responsibilities) salaries with federal subset.

If these federal grant program dollars are jeopardized or reduced, it could have direct impact on these CIP staffing investments. This vulnerability was further reinforced by many respondents in the open narrative question at the end of the survey, Table 1 (Question 18, N=52) where respondents were asked to provide one thing that could be done in their jurisdiction to improve their CIP program. Of the 52 respondents to this question, 11 respondents (21.15 percent) specifically cited the need for more and/or dedicated funding. Please see Figure 23.

From a state and local governmental program perspective and based on respondents' survey responses, CIP responsibilities appear to be a collateral duty assigned to organizational components not fully dedicated to the CIP mission, with minimal programmatic staffing. This was very clearly indicated by the survey response data of multiple questions wherein 28 of 47 respondents (59.57 percent) indicated one or two fulltime staff members assigned to CIP responsibilities. Almost half the respondents to Question 22 (21 of 47 respondents (44.68 percent)) indicated that where there is fulltime programmatic staffing, it appears to be one fulltime staff member (Figures 13 and 14). Seven respondents (14.89 percent) indicated two fulltime staff members, and almost a quarter of respondents (11 of 47 respondents (23.40 percent)) indicated a range of three to seven fulltime staff members maintained. Eight respondents (17.02 percent) further indicated greater than 10 fulltime staff members assigned to CIP responsibilities.

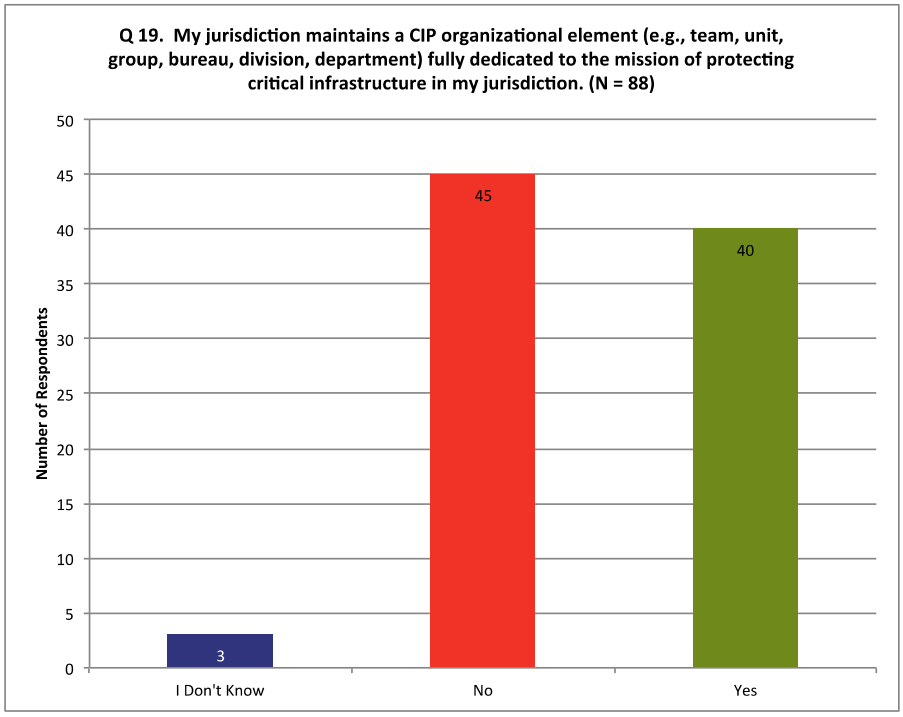


Figure 13. Respondents' jurisdiction maintains a CIP organizational element fully dedicated to CIP protection mission.

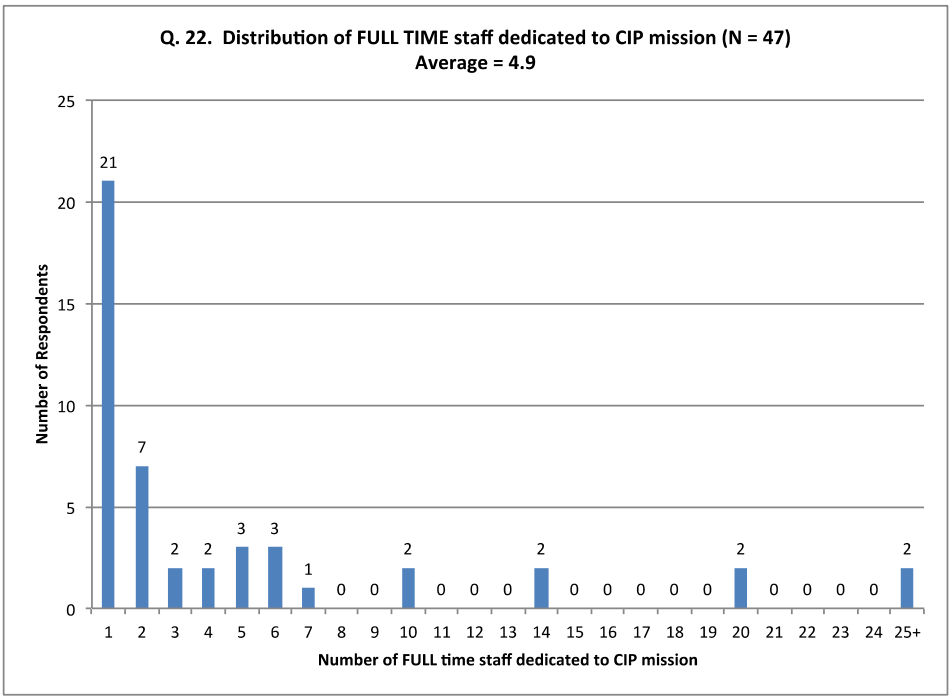


Figure 14. Distribution of full time staff dedicated to the CIP mission.

Responses did not appear to vary greatly when cross-analyzed against CIP practitioner/partner status, jurisdiction type, or qualified jurisdiction. A data anomaly was recognized in Figure 15 regarding Region 5, wherein 25 percent of respondents indicated they had fulltime staff dedicated to the CIP mission and when asked how many staff, Region 5 respondents indicated an average of 7.3 fulltime staff members. The Region 5 average of 7.3 staff members is well above the overall respondent average of 4.9 full time staff (indicated by Figure 16).

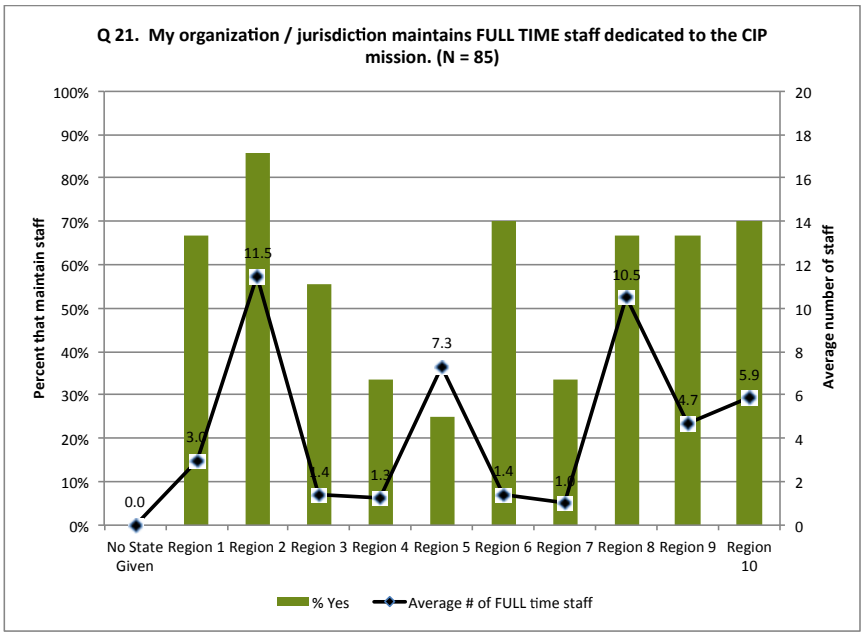


Figure 15. Percentage of respondents by federal FEMA region that indicated they have fulltime staff and the average number of the fulltime staff reported.

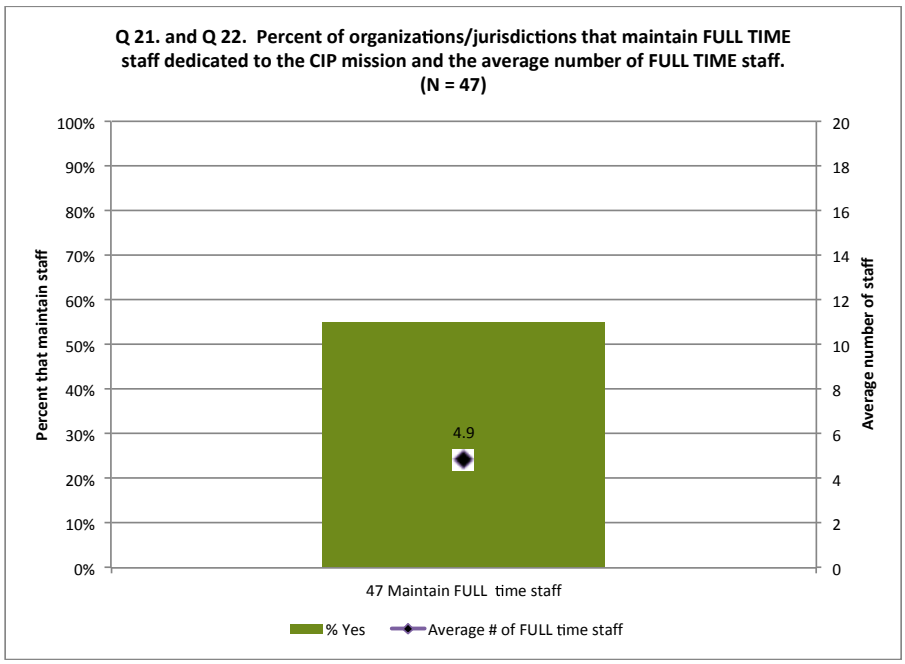


Figure 16. Percentage of respondents that indicated fulltime CIP staff are maintained by their organization/jurisdiction and the average number of full time staff indicated.

Regions 4, 6, and 7 were below the overall average, indicating 1.3, 1.4 and 1.0 fulltime staff respectively. Region 2 appears to have the most dedicated fulltime staff as indicated by 86 percent of Region 2 respondents and is also well above the average number of fulltime staff maintained with an average Region 2 report of 11.5 staff members. Respondents indicated that their organization or jurisdiction also maintained an average of 4.3 part-time staff members dedicated to the CIP mission (see Figure 17). Regions 1, 4, and 5 had the greatest number of jurisdictions that maintain part-time staff, and Regions 1, 4, and 9 had the greatest numbers of part-time staff members assigned within the jurisdictions in each region. Of note, as Figure 18 indicates, Regions 3, 6, 7, and 8 reported no part-time staff member assignments. Though 87.50 percent of respondents indicated five or less part-time staff assigned in their jurisdiction, two outlier data points were present: two respondents indicated 10 part-time staff, and one respondent indicated 25+ part-time staff members assigned (Figure 19).

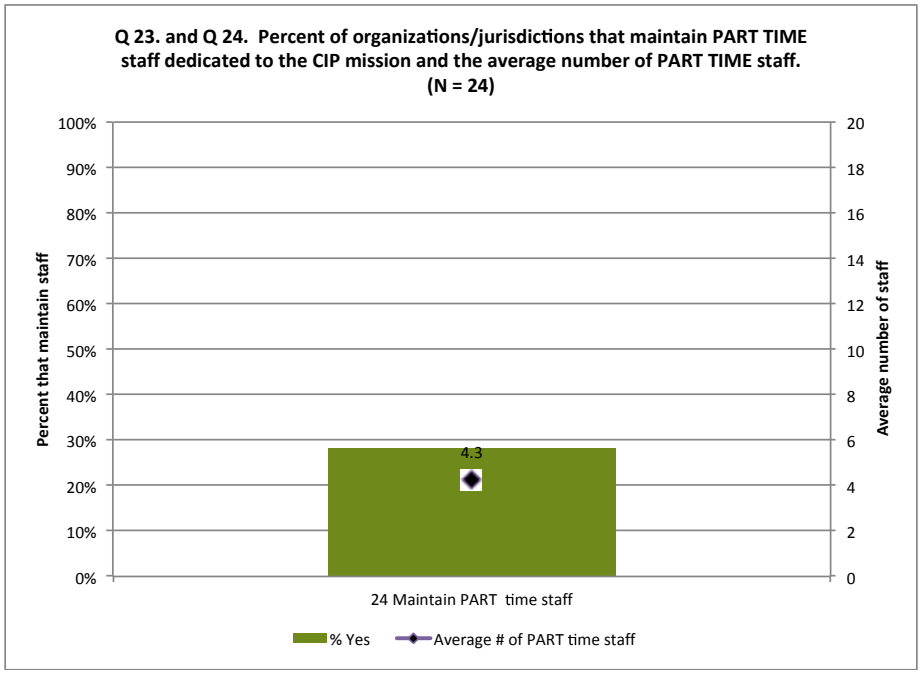


Figure 17. Percentage of respondents that indicated part time CIP staff are maintained by their organization/jurisdiction and the average number of part time staff indicated.

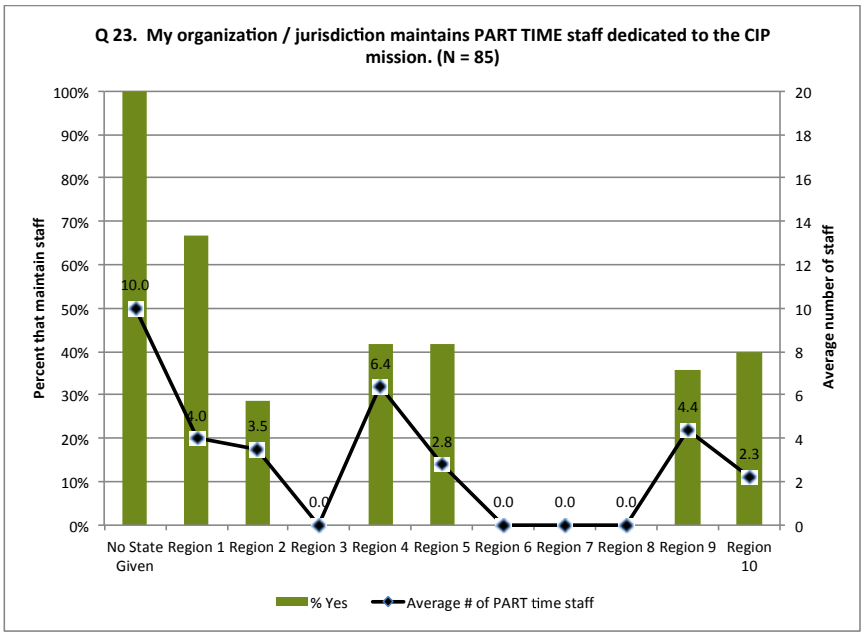


Figure 18. Percentage of respondents by federal FEMA region that indicated they have part-time staff and the average number of the part-time staff reported.

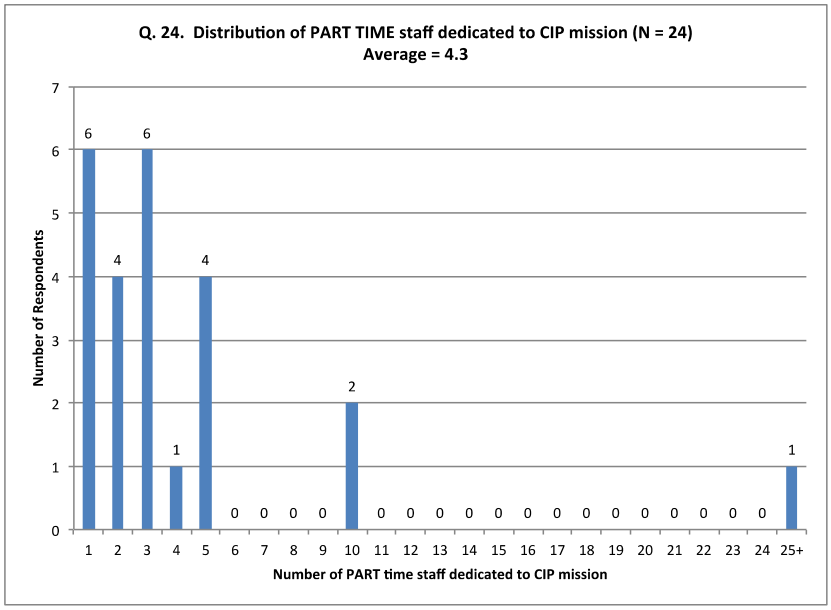


Figure 19. Distribution of part time staff dedicated to the CIP mission.

As indicated by Figure 20, respondents generally disagreed when asked if their jurisdiction's CIP program was managed by an organizational component

entirely dedicated to CIP as its core mission; 53 of 85 respondents (62.35 percent) expressed negative sentiment, and 31 of 85 respondents (36.47 percent) expressed positive sentiment (Question 29: Average 2.95, N=85). When cross-analyzed by CIP practitioner/partner status, jurisdiction type, and federal FEMA regions (see Figures 20A–20F in Appendix C), respondents from county/parish levels of government disagreed more (almost 80 percent) than those respondents from local (city/town/village/municipal) and state levels of government who both disagreed almost 60 percent of the time. Respondents from federal FEMA Regions 4, 5, and 7 almost entirely disagreed. The data indicates a clear lack of dedicated CIP organizations at the state and local levels. This becomes important in the context of the numerous and varied expectations placed upon the community.

This data was inversely supported by data in Figure 21. Respondents were asked to indicate if they felt the CIP program in their jurisdiction was managed as a collateral responsibility by an organizational component whose core mission was not critical infrastructure protection (Question 30: Average 3.93, N=84). Respondents generally agreed that this was the case. When cross-analyzed by CIP practitioner/partner status, jurisdiction type, and federal FEMA regions, respondents from FEMA Regions 1, 2, and 8 disagreed the most, and respondents from Region 7 agreed 100 percent of the time.

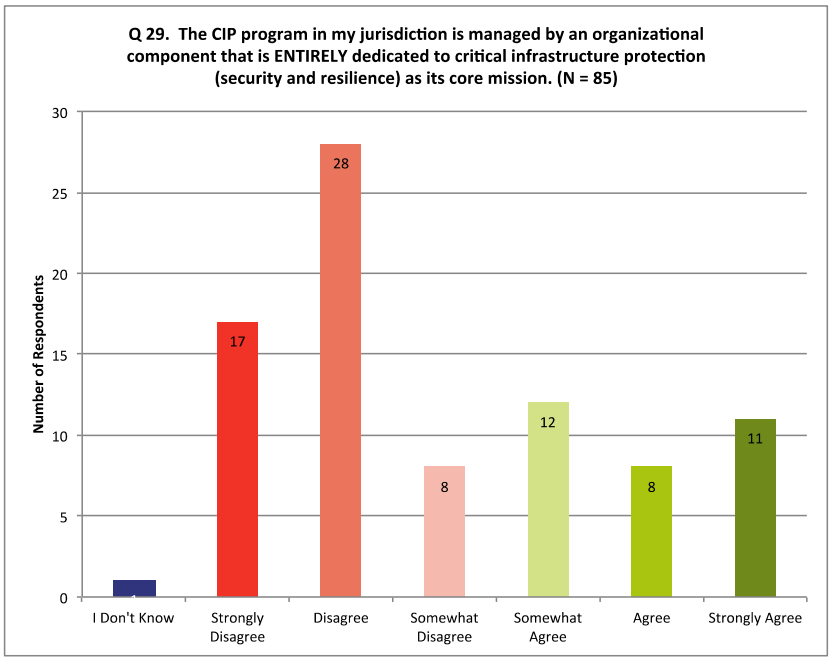


Figure 20. Respondents' perception that their jurisdiction's CIP program is managed by an organizational component entirely dedicated to CIP (security and resilience) as its core mission.

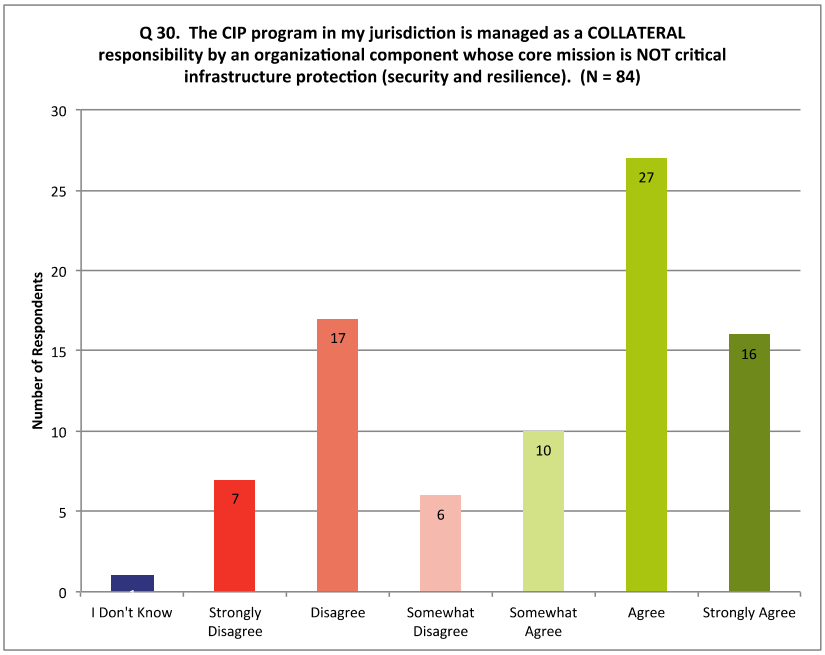


Figure 21. Respondents' perception that their jurisdiction's CIP program is managed as a collateral responsibility by an organizational component whose core mission is not CIP (security and resilience).

CIP organizations with more robust organizational or programmatic staffing do exist, but they appear to be more the exception than the standard. When asked whether the CIP program or organization in their jurisdiction was adequately staffed, most respondents answered overwhelmingly negative (Question 25: Average 2.62, N=86) that their CIP program or organization was adequately staffed, though a pocket of positive respondents did exist (see Figure 22). Cross analysis of response data (see Figures 22A–22H in Appendix C) by CIP practitioner/partner status, jurisdiction type, and federal FEMA regions showed no remarkable inconsistencies. Respondents from federal FEMA Regions 6 and 7 disagreed 100 percent of the time. Given the clear expectation among many for this professional community to coordinate and share information with public safety professionals as well as asset owners and operators in their jurisdiction,[58] perhaps the indication of inadequate staffing should be expected.

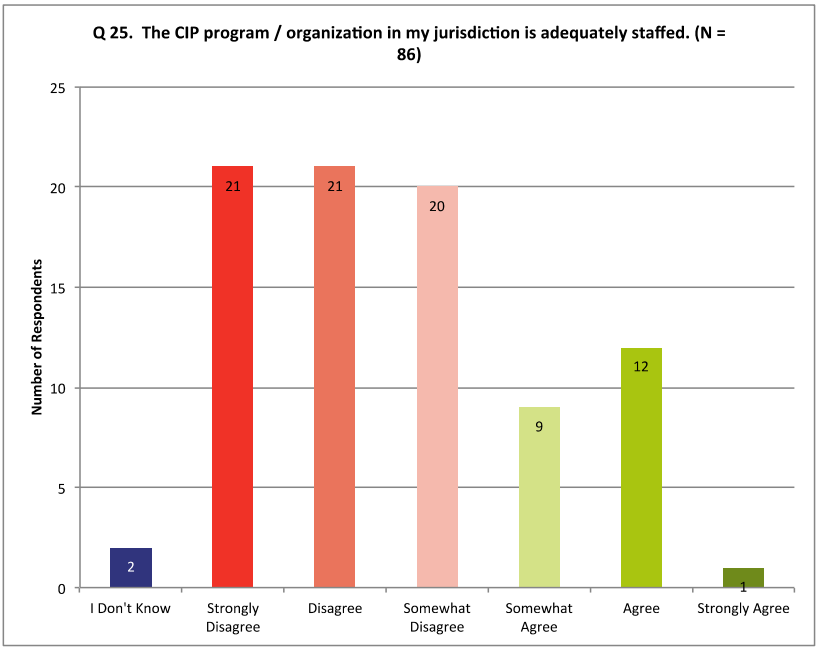


Figure 22. Respondents' perception that the CIP program/organization their jurisdiction is adequately staffed.

[58] U.S. Department of Homeland Security, *Homeland Security Presidential Directive 7*; White House, *The National Strategy for The Physical Protection*, x.

Of note, the view of inadequate staffing appears also to transcend a respondent's years of experience as either a CIP practitioner or partner. Respondents across all experience ranges indicated a 70 percent to 80 percent disagreement when asked if their CIP program or organization was adequately staffed (see Figures 23 and 24). Whether reality or perception that CIP programs are understaffed, the issue warrants further research or more in depth exploration and analysis. If left unchecked, the views may lead to a breakdown of program efficacy or morale.

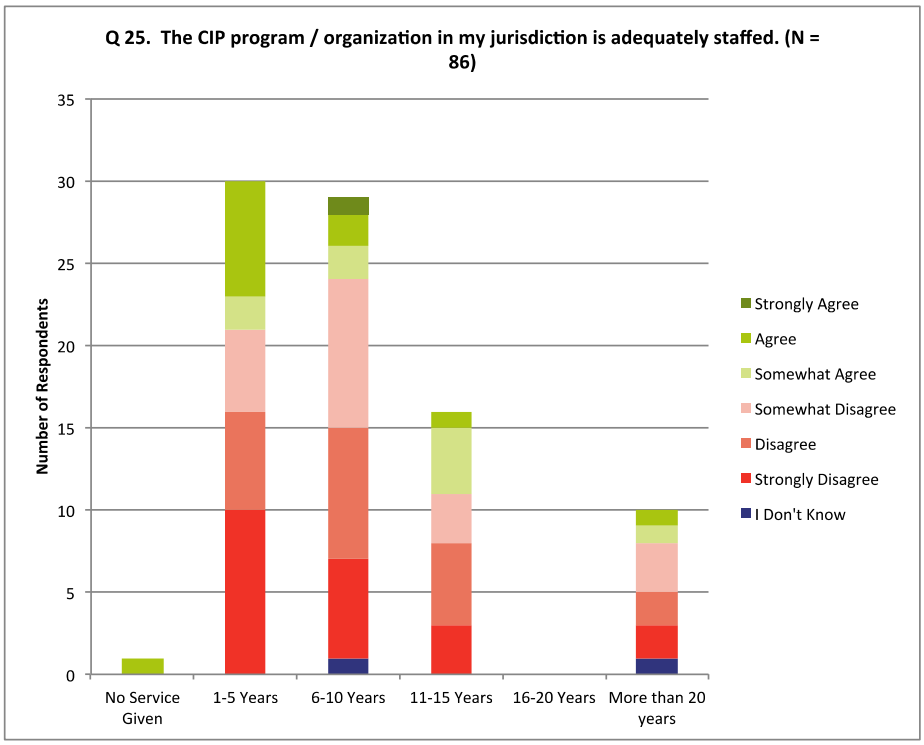


Figure 23. Figure 22 cross-analyzed by respondents' years of experience.

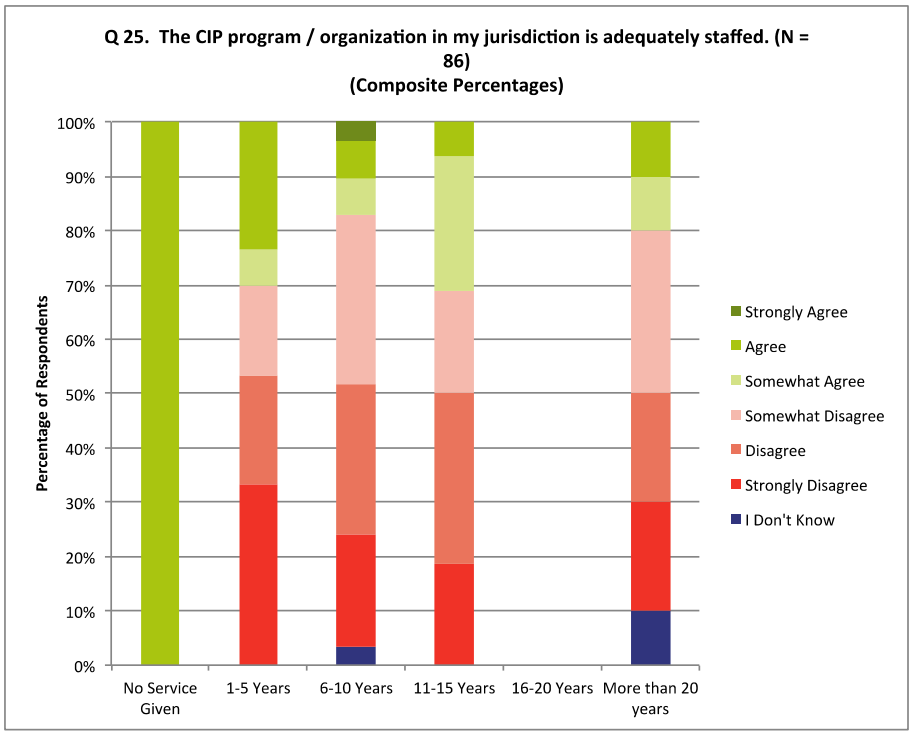


Figure 24. Composite percentages of Figure 23.

This real or perceived need for additional staff was also clearly reinforced by many respondents in the open narrative question at the end of the survey. With a word cloud, Figure 25 visually depicts the narrative provided by respondents in Question 48, in which respondents were asked to provide one thing that could be done in their jurisdiction to improve their CIP program (the word size illustrates the word weight by frequency). Just over one-third of the 52 respondents to this question, 18 of 52 respondents (34.61 percent) specifically cited the need for more and/or dedicated CIP program staff.

Figure 25. Table 1, Question 48 narrative response word cloud (N=52).

As illustrated by Figure 26, most respondents indicated that the CIP program staff in their jurisdiction had a very strong productive working relationship with the U.S. Department of Homeland Security protective security advisor (PSA) assigned to their jurisdiction (Question 14: Average 4.93, N=91). In addition, 79 of 91 respondents (86.81 percent) indicated a positive feeling of their jurisdictions working relationship. Notably, almost half of all respondents to this question (45 of 91 respondents (49.45 percent)) strongly agreed that their jurisdiction maintained a productive working relationship with the PSA assigned to their jurisdiction. This feeling appears to be generally universal when cross-analyzed against supporting data (see Figures 26A–26F in Appendix C) of CIP practitioner/partner status, jurisdiction type, and federal FEMA region. This very strong productive working relationship is a very positive reflection of the PSA program and certainly indicates great collaboration and partnership between professionals across the levels of government. It could also indicate a level of underlying programmatic dependence on the federal government and the PSA program to deliver local CIP programs. If this dependence exists and if it is

functional, there is nothing inherently wrong with programmatic dependence. However, the existence or level of programmatic dependence on the PSA program by more local jurisdictions should be better understood by policy makers before future modifications or reductions are made to the PSA program.

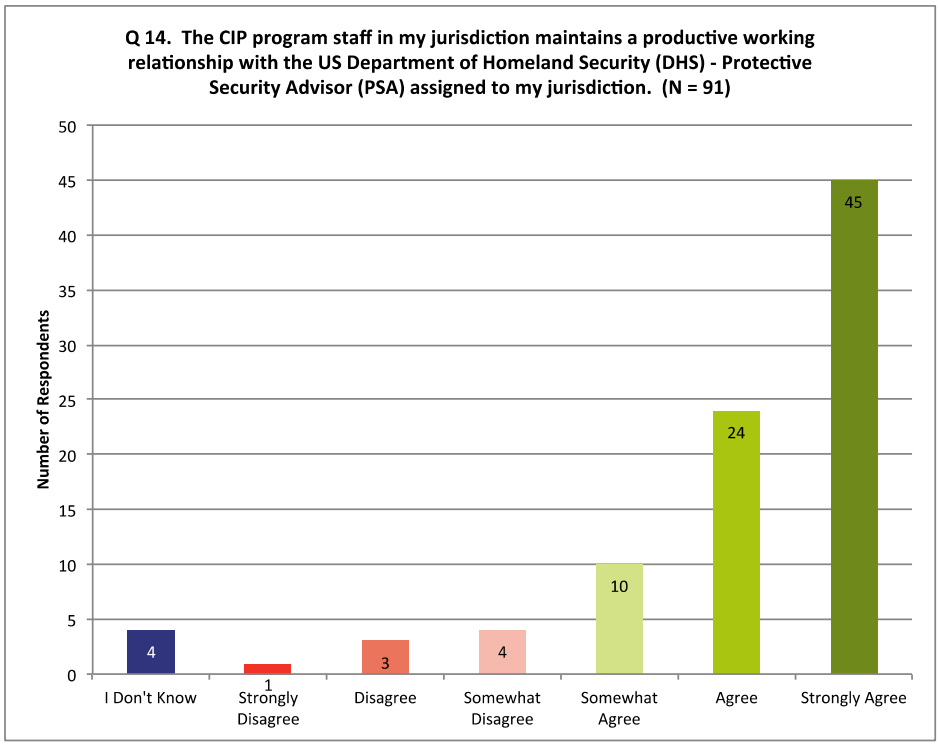


Figure 26. Respondents' perspective that CIP program staff in their jurisdiction maintains a productive working relationship with the DHS protective security advisor assigned to their jurisdiction.

Figures 27 and 28 show that most respondents were generally neutral (Question 38: Average 3.61, N=83 and Question 39: Average 3.59, N=82) about whether the CIP mission and organization in their jurisdiction was well understood by stakeholders. This neutrality appears consistent when responses are cross-analyzed against CIP practitioner/partner status, jurisdiction type, and federal FEMA region (see Figures 27A–27F and 28A–28F in Appendix C). This perhaps is in part or in full why local leaders have not invested more directly in

their CIP programs or organizations—perhaps the real or perceived need to do so is not clear and/or well understood.

The neutral view of respondents indicating a lack of mission and organizational clarity by stakeholders may indicate a lack of clear role or mandate or the ability to communicate effectively the role or mandate. The lack of stronger understanding by stakeholders could hinder cooperation or retard coordination amongst partners.

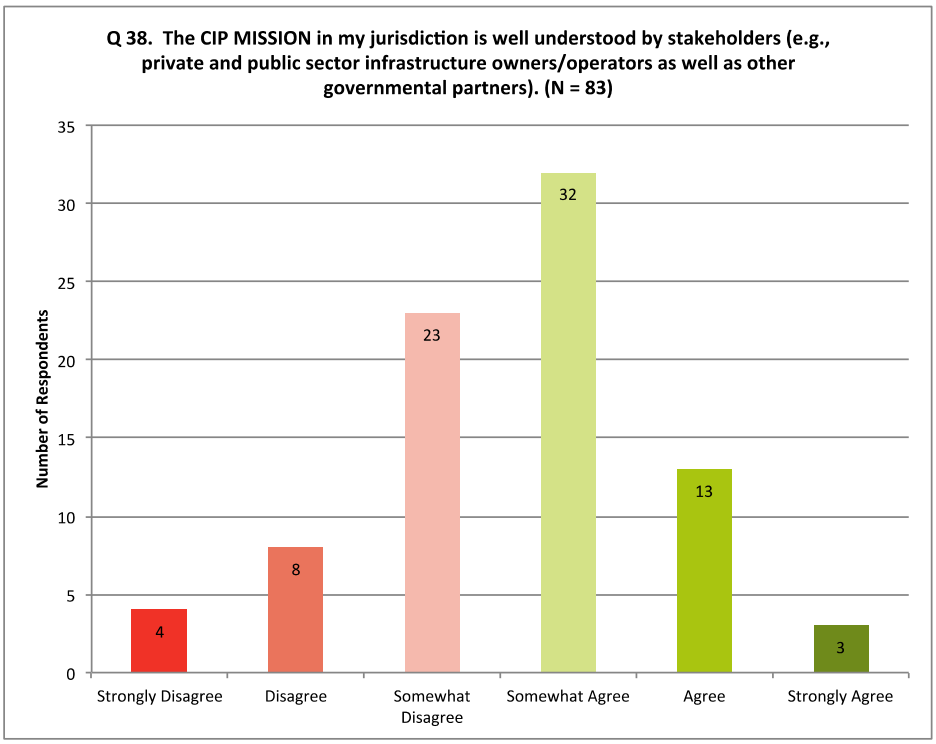


Figure 27. Respondents' perspective on whether the CIP mission in their jurisdiction is well understood by stakeholders.

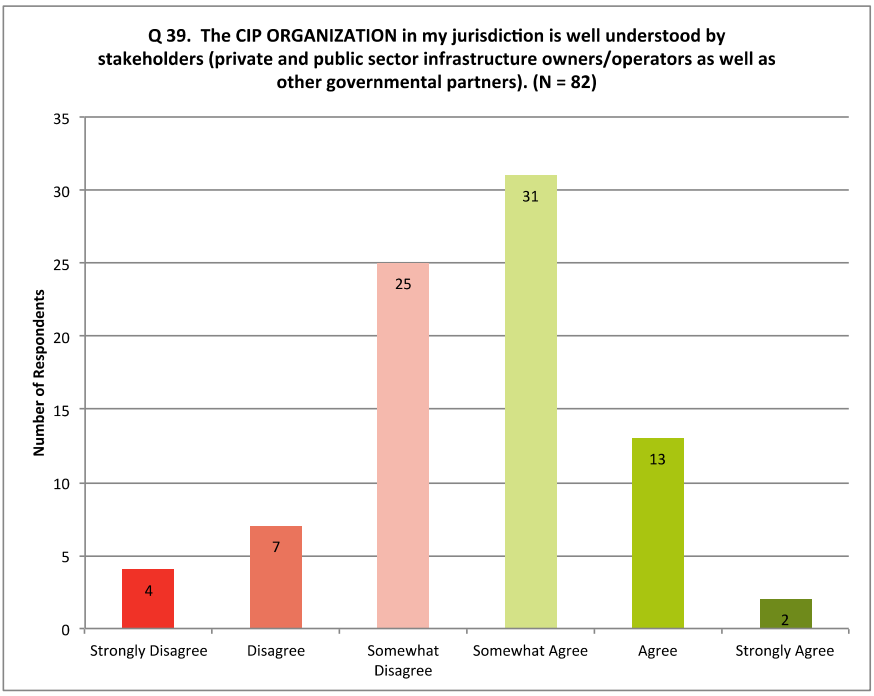


Figure 28. Respondents' perspective on whether the CIP organization in their jurisdiction is well understood by stakeholders.

As further demonstrated by Figures 29–31, most respondents were generally neutral to negative (Question 43: Average 3.12, N=83; Question 44: Average 3.55, N=83; and Question 45: Average 3.64, N=83) about whether the CIP mission was fully implemented, implemented well and well managed in their jurisdiction. These responses may indicate respondents' tactical lack of understanding of their jurisdiction's CIP mission or awareness of programmatic development and implementation. It could also indicate a tactical lack of programmatic or organizational maturity in the jurisdiction. This issue also warrants additional research, exploration, and analysis.

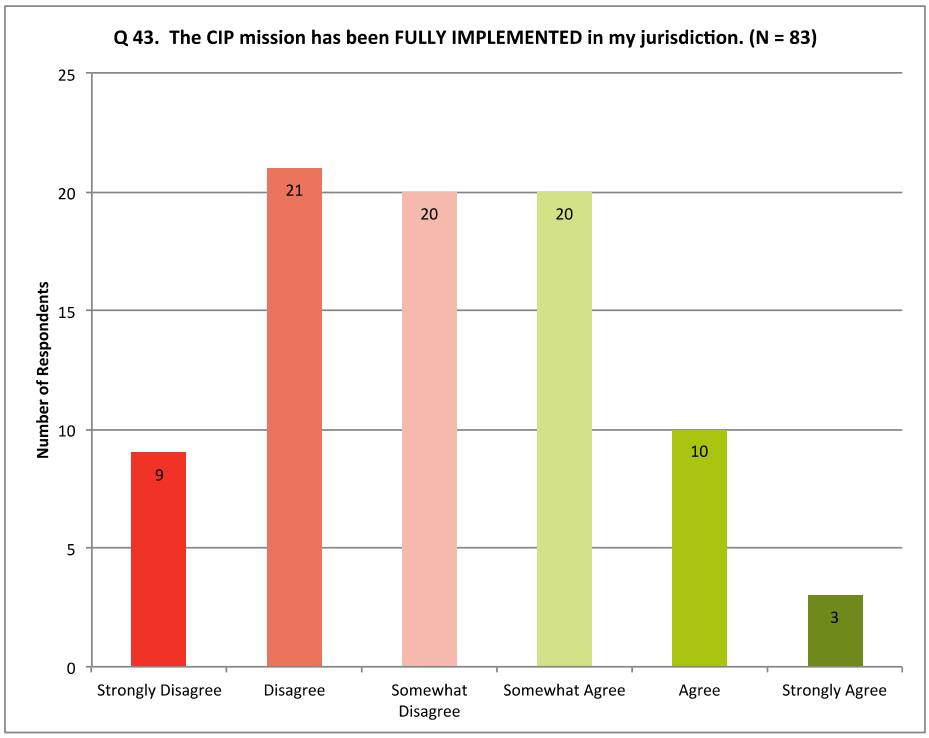


Figure 29. Respondents' perspective on whether the CIP mission in their jurisdiction has been fully implemented.

The expressed lack of mission and organizational clarity noted earlier may also be impeding mission implementation or fostering a clear and generally neutral perception regarding CIP mission implementation. Figure 30 specifically and clearly indicates this neutral sentiment of respondents. (Question 44: Average 3.55, N=83).

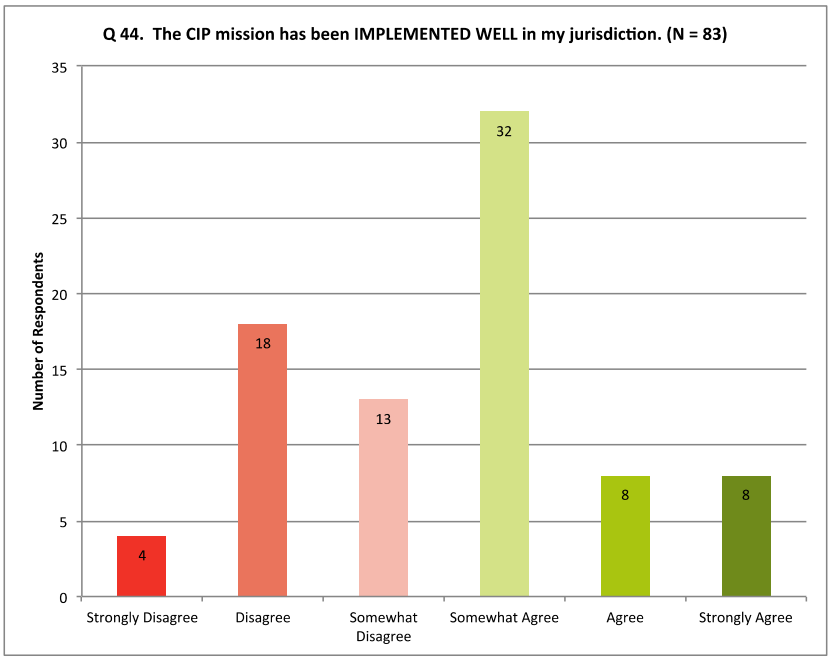


Figure 30. Respondents' perspective on whether the CIP mission in their jurisdiction has been implemented well.

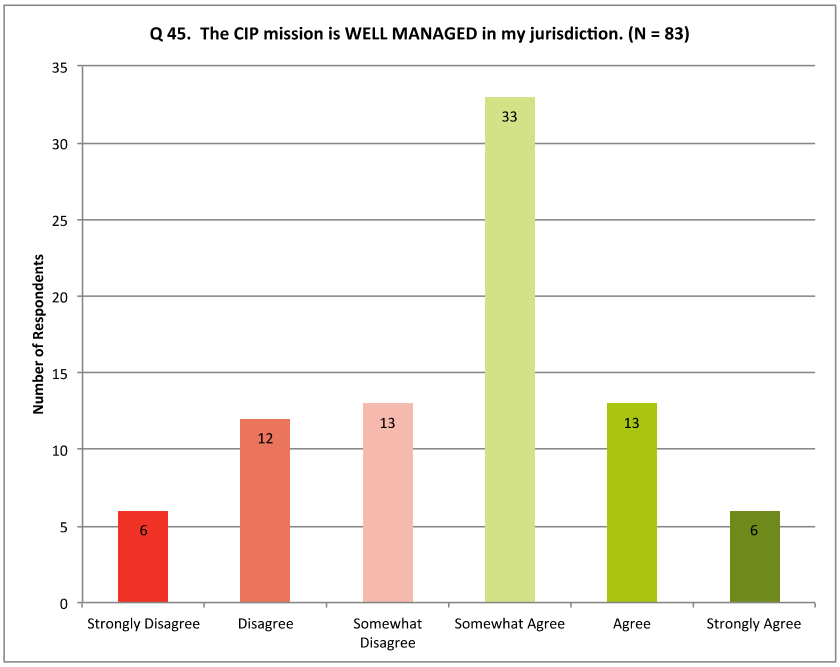


Figure 31. Respondents' perspective on whether the CIP mission in their jurisdiction is well managed.

On the whole, the neutral to negative views expressed by respondents on whether the CIP mission in their jurisdiction is fully implemented, implemented well, and managed well could provide a real or perceived obstacle to future programmatic maturity. Respondents appear to be generally torn or neutral on several fronts. Notably, in Figure 32, respondents were divided on whether their chief executives or governing bodies have enacted effective CIP related executive orders and legislation related to CIP and/or CIP program authorities or requirements (Question 11: Average 3.62, N=91). Additionally, 38 of 91 respondents (41.76 percent) indicated some level of disagreement to this question, while 53 of 91 respondents (58.24 percent) indicated a level of agreement. Strongly disagree and strongly agree both had the fewest number of respondents (nine each). Cross-analysis by qualified jurisdiction demonstrated generally consistent answers with the exception of rural respondents that indicated 100 percent disagreement; it should be noted that the fewest respondents were from rural jurisdictions.

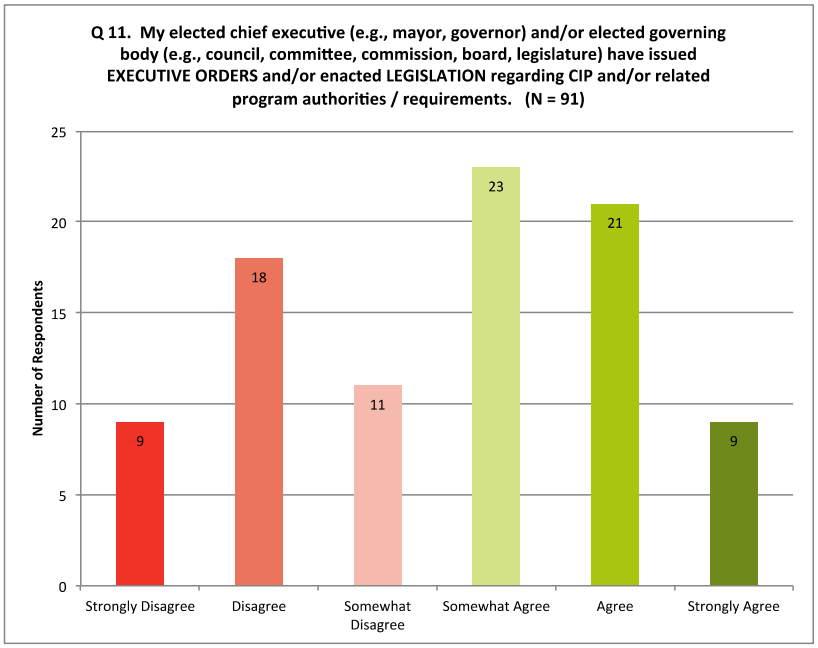


Figure 32. Respondents' perspective on whether their chief executive or governing body has issued executive orders or enacted legislation regarding CIP and/or related program authorities / requirements

Figures 33 and 34 appear to indicate that respondents feel equally torn or neutral on basic program management functions such as whether effective performance measures (Question 15: Average 3.52, N=91) and well-defined programmatic goals, objectives, and related business process exist in their jurisdictions (Question 40: Average 3.57, N=82). Cross-analysis of these responses against qualified jurisdictions and jurisdiction type were generally consistent and showed one note of interest. Figures 35 and 36 indicate respondents from rural and rural-suburban jurisdictions disagreed the most at a rate of 50 percent and 70 percent respectively. Of interest, when given the risk as they know it or understand it in their jurisdiction, Figure 37 indicates that respondents perceptions were also torn or neutral on whether every reasonable measure had been taken to assure critical infrastructure is well protected (Question 46: Average 3.47, N=83). Cross-analysis of supporting data by organization type, qualified jurisdiction, and jurisdiction type (see Figures 37A–37F in Appendix C) showed response variation by the respondents organization type and qualified jurisdiction; responses by jurisdiction type were generally consistent.

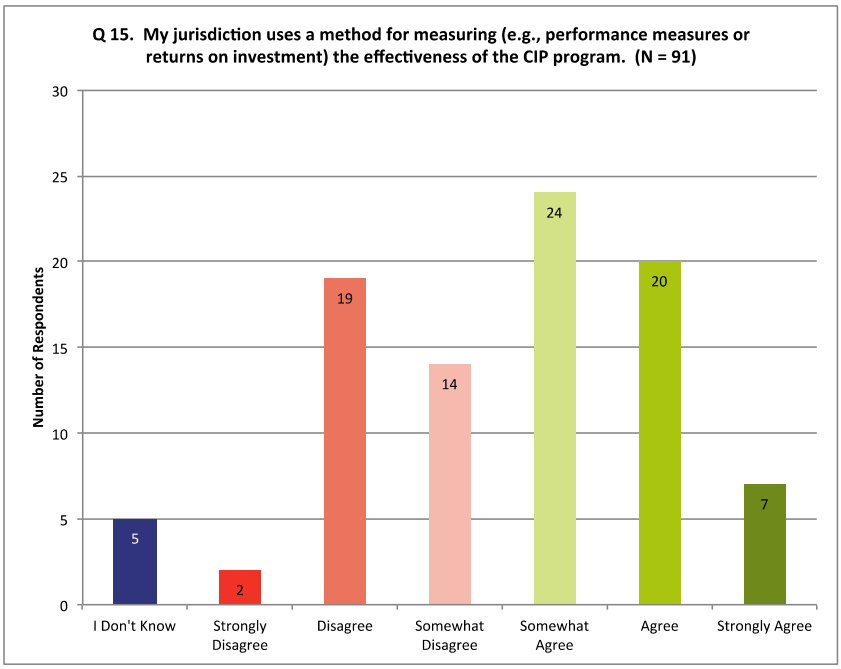


Figure 33. Respondents' perspective on whether their jurisdiction uses a method for measuring the effectiveness of their CIP program.

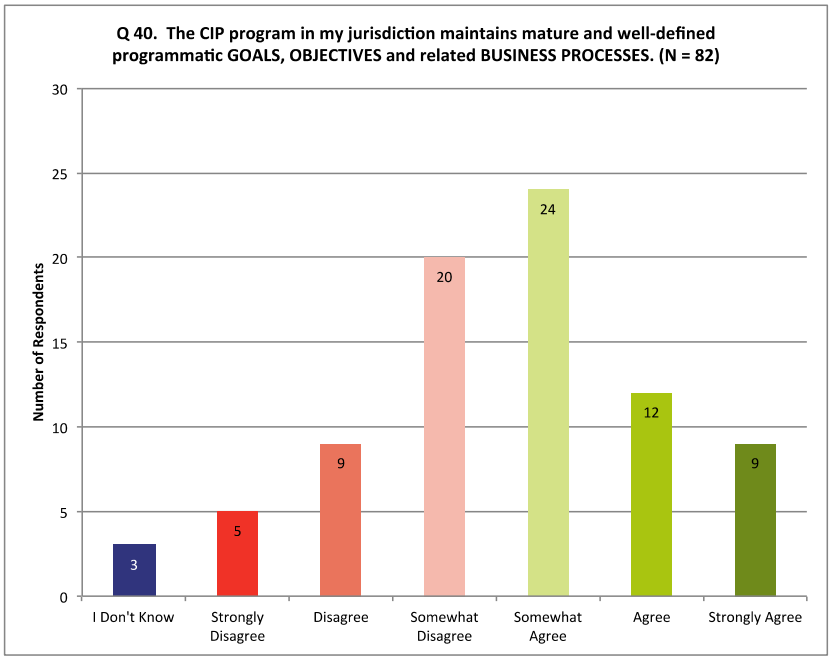


Figure 34. Respondents' perspective on whether the CIP program in their jurisdiction maintains mature and well-defined programmatic goals, objectives, and related business process.

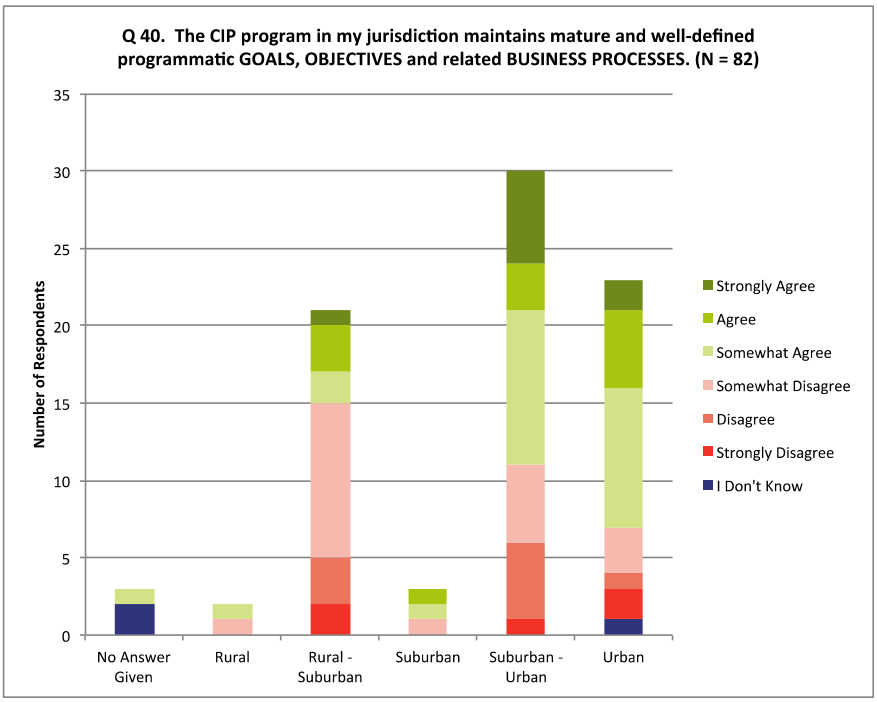


Figure 35. Figure 34 Cross-analyzed by respondents qualified jurisdiction.

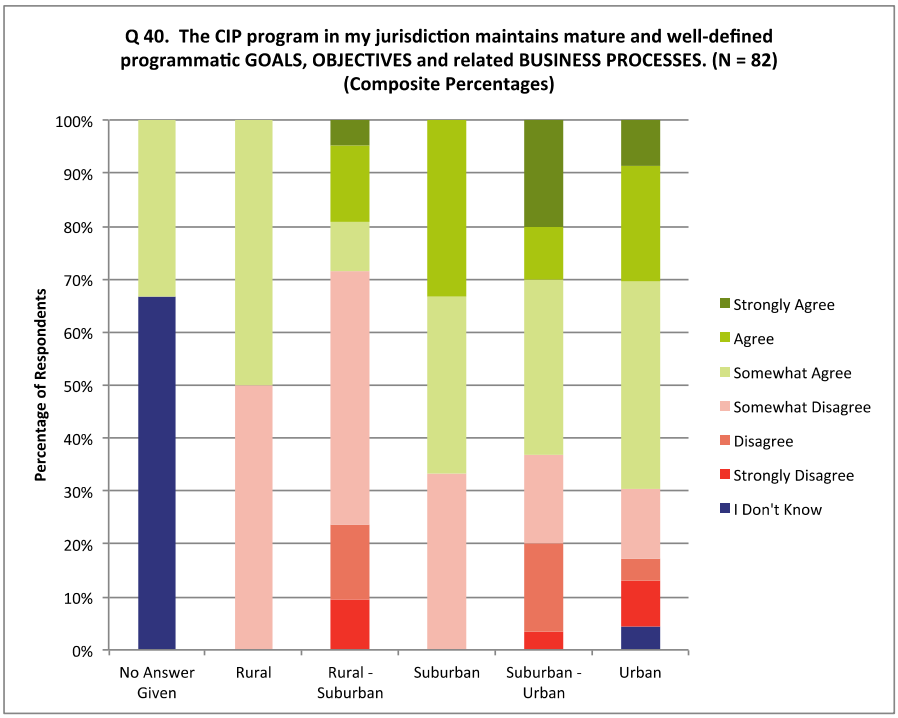


Figure 36. Composite percentages of Figure 35.

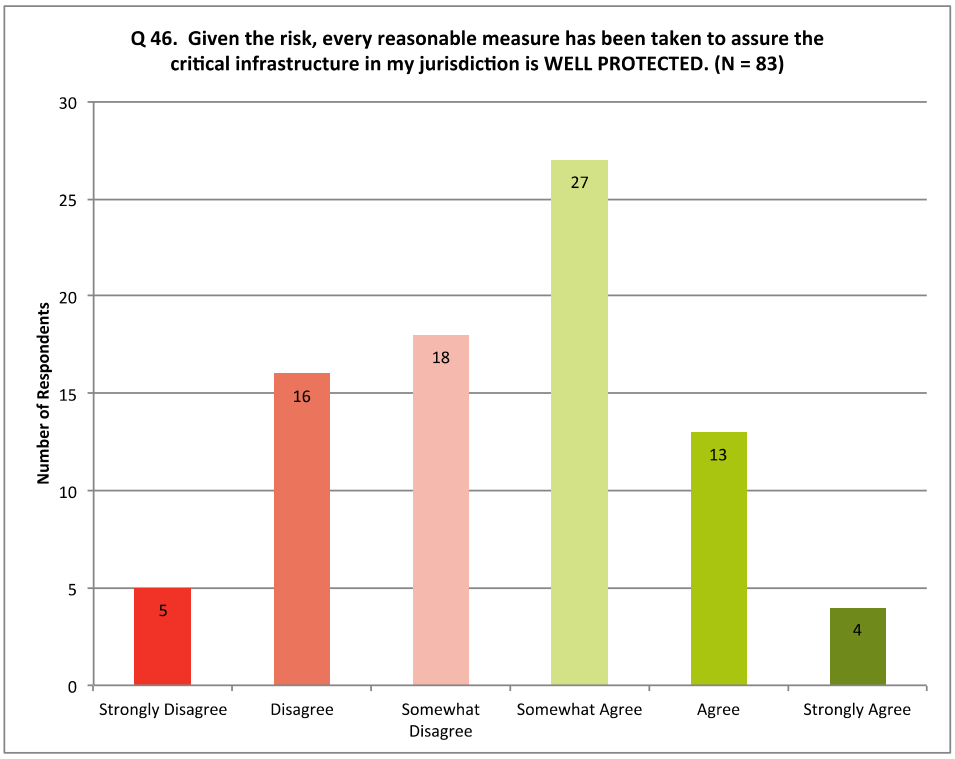


Figure 37. Given the known or understood jurisdictional risk, respondents' perspective on whether every reasonable measure has been taken to assure critical infrastructure in their jurisdiction is well protected.

Also of note as illustrated by Figure 38 (Question 13: N=91), respondents indicated that almost two-thirds (64.83 percent) of jurisdictions maintain a CIP all-hazard strategic plan, and just under one-third (28.57 percent) of jurisdictions do not appear to have a recognized strategic plan in place. Respondents' data indicates that the northeast (FEMA Regions 1 and 2) appears to have the greatest number of strategic plans in place (see Figures 38C and 38D in Appendix C).

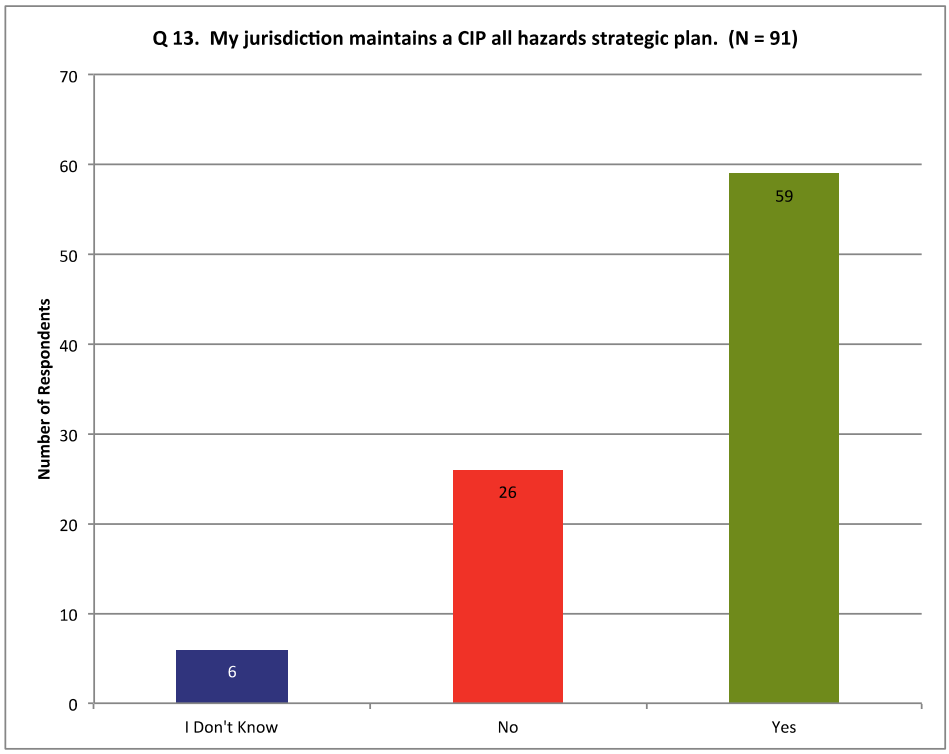


Figure 38. Respondents understanding or view on whether their jurisdiction maintains a CIP all hazard strategic plan.

Despite the potential lack of tactical program understanding or maturity, as shown by Figures 39 and 40, strategically, most respondents (68 of 90 respondents (75.56 percent) and 81 of 91 respondents (89.01 percent) respectively) indicated positively that CIP has become (Question 9: Average 4.18, N=90) or should become and be maintained as a discrete professional discipline (Question 10: Average 4.91, N=91). Conversely and respectively, 22 of 90 respondents (24.44 percent) and 10 of 91 respondents (10.99 percent) expressed negative sentiment that CIP has become or should become or be maintained a professional discipline. Cross-analysis of support data (see Figures 39A–39H in Appendix C) by CIP practitioner/partner status, organization type, jurisdiction type, and federal FEMA region generally supported this thinking with some variations indicated.

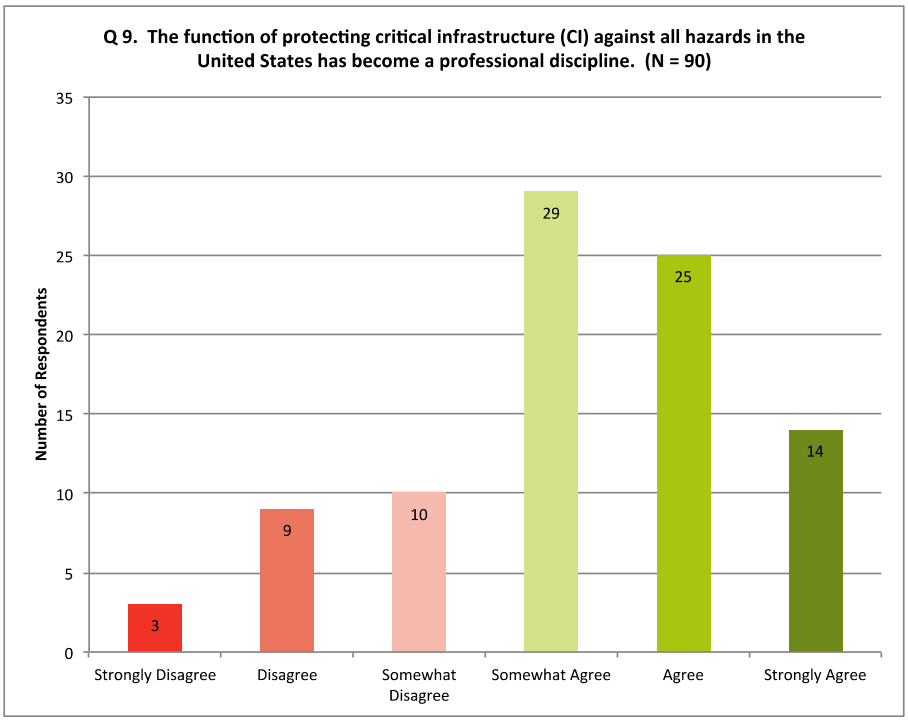


Figure 39. Respondents' perspective on whether the function of protecting critical infrastructure against all hazards has become a professional discipline.

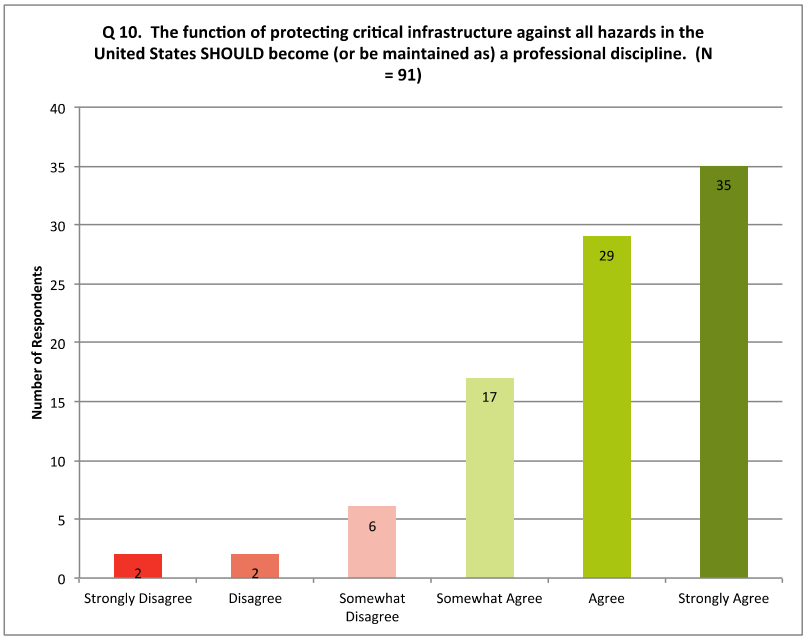


Figure 40. Respondents' perspective on whether the function of protecting critical infrastructure against all hazards should become or be maintained as a professional discipline.

As indicated by Figure 41, most respondents (87 of 90 respondents (96.66 percent)) also clearly felt that their jurisdictions do strategically recognize and utilize concepts outlined in the *National Infrastructure Protection Plan* (Question 12: Average 4.92, N=90). Cross analysis of support data (see Figures 41A–41D in Appendix C) by jurisdiction type and federal FEMA region reinforced broad support of the NIPP. It should be noted that very small pockets of disagreement in FEMA Regions 5 and 6 and among state respondents was seen.

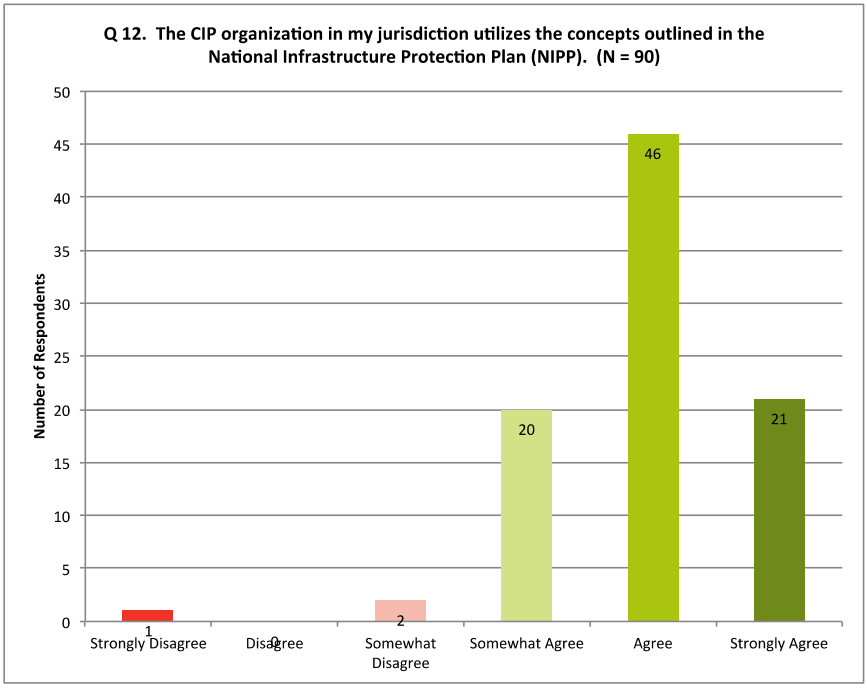


Figure 41. Respondents' perspective on whether the CIP organization in their jurisdiction utilizes the concepts outlined in the *National Infrastructure Protection Plan*.

A large majority of respondents (77 of 86 respondents (89.53 percent)), as illustrated in Figure 42, indicated positive feeling that the CIP/risk management mission should be more closely aligned to the mitigation and preparedness mission space of emergency management (Question 20: Average 4.69, N=86). As further illustrated in Figure 42, some respondents (nine of 86 respondents (10.46 percent)) indicated negative feeling to this closer mission space alignment. Cross-analysis of support data by CIP practitioner/partner status,

organization type, jurisdiction type, and federal FEMA regions (see Figures 43–46 below and Figures 42A and 42B in Appendix C), specifically Figures 43 and 44, indicated generally consistent and broad support of a closer mission space alignment. As was previously illustrated in Figure 4, approximately one-third (32 of 91 respondents (35.16 percent)), self-identified their organizations affiliation as emergency management.

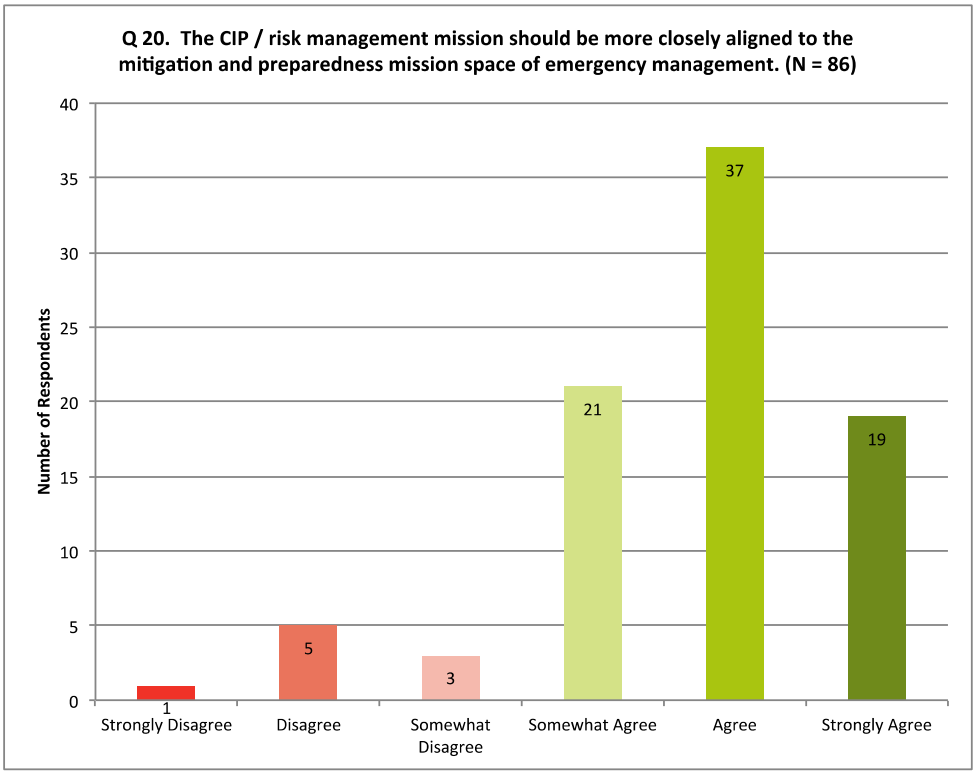


Figure 42. Respondents' perspective on whether the CIP / risk management mission should be more closely aligned to the mitigation and preparedness mission space of emergency management

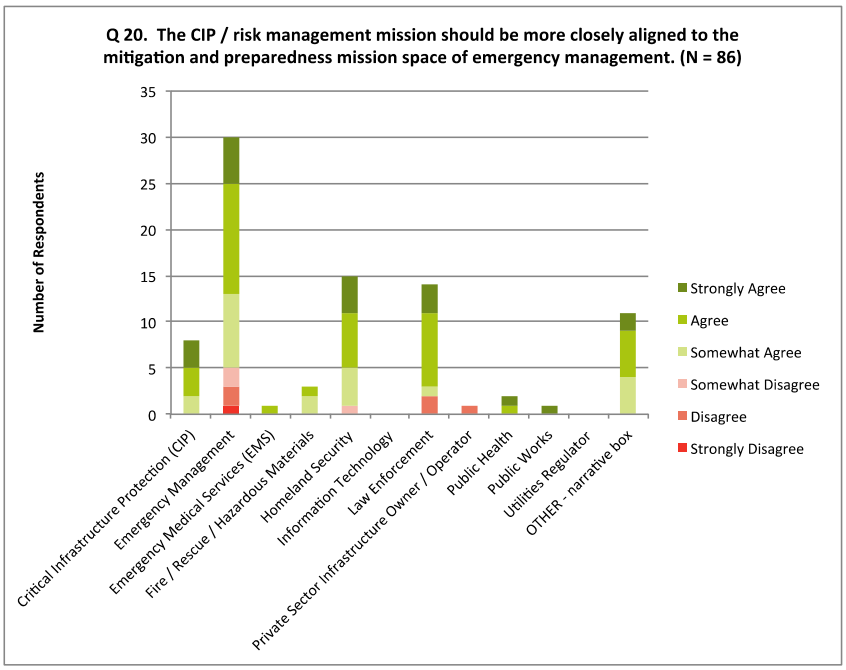


Figure 43. Figure 42 cross-analyzed by respondents federal FEMA region.

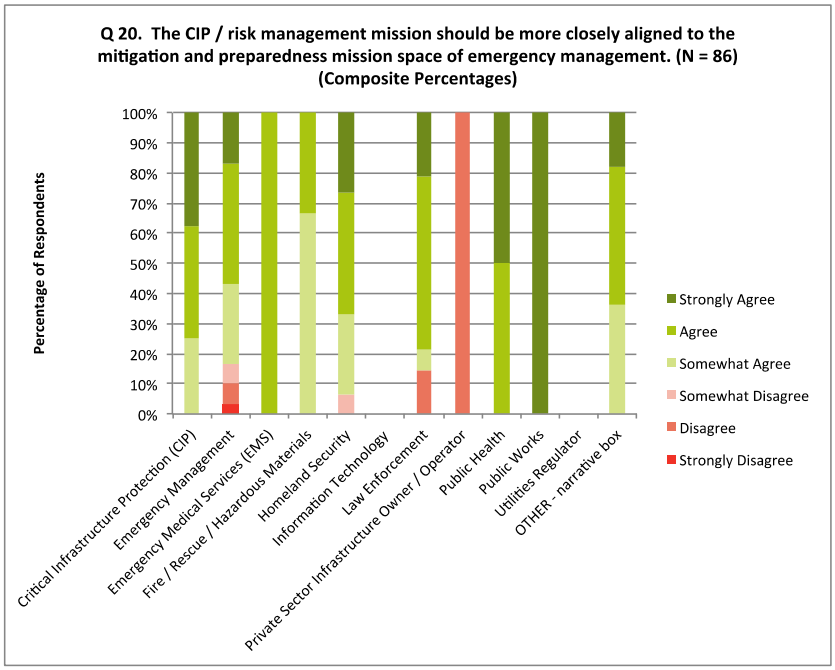
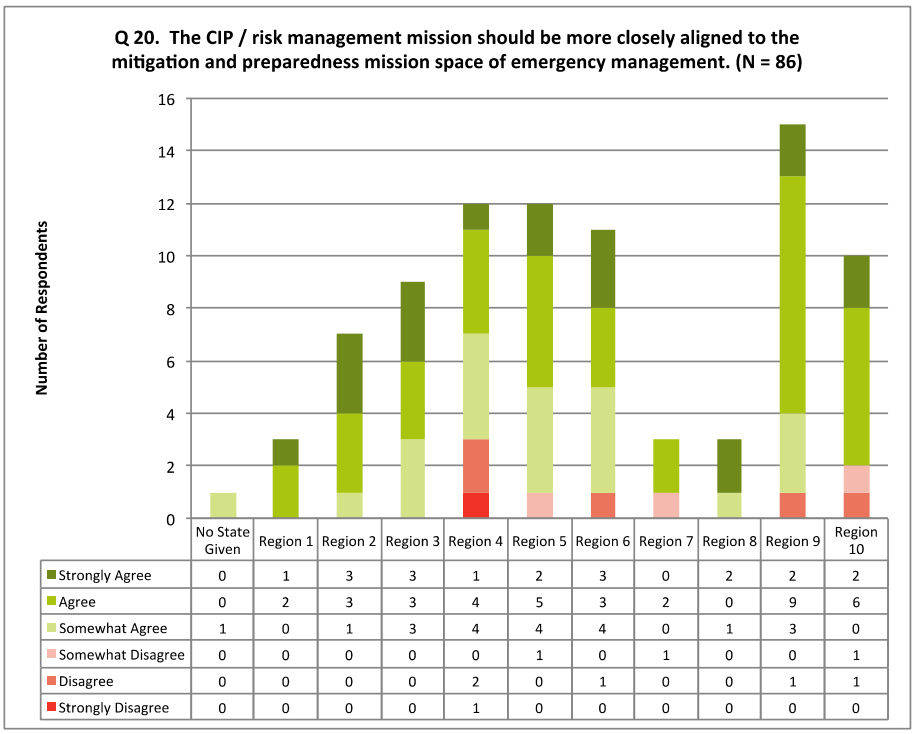
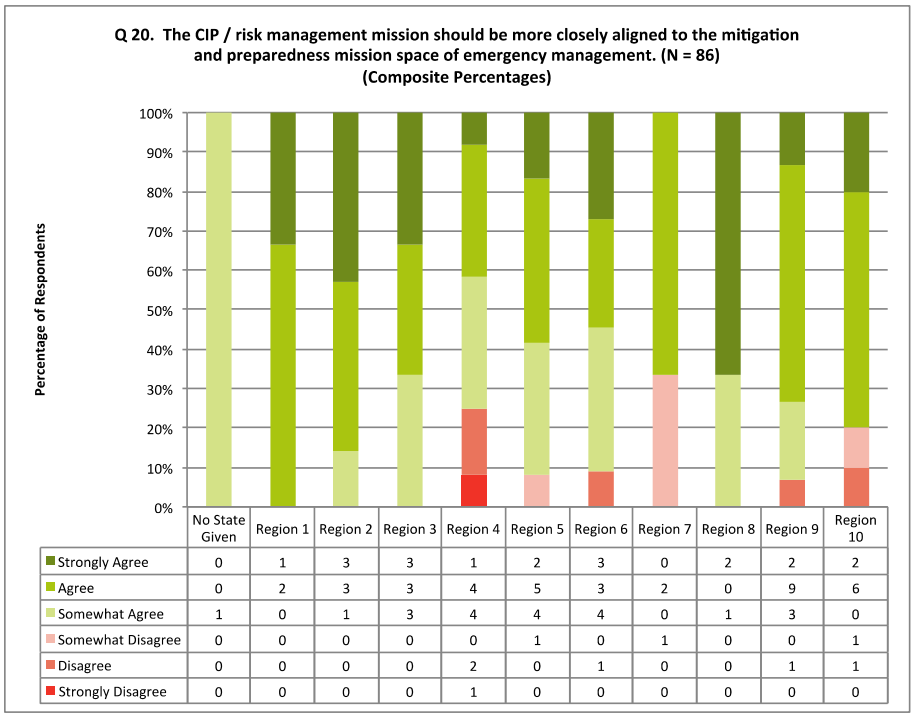


Figure 44. Composite percentages of Figure 43G.



	No State Given	Region 1	Region 2	Region 3	Region 4	Region 5	Region 6	Region 7	Region 8	Region 9	Region 10
Strongly Agree	0	1	3	3	1	2	3	0	2	2	2
Agree	0	2	3	3	4	5	3	2	0	9	6
Somewhat Agree	1	0	1	3	4	4	4	0	1	3	0
Somewhat Disagree	0	0	0	0	0	1	0	1	0	0	1
Disagree	0	0	0	0	2	0	1	0	0	1	1
Strongly Disagree	0	0	0	0	1	0	0	0	0	0	0

Figure 45. Figure 42 cross-analyzed by respondents federal FEMA region.



	No State Given	Region 1	Region 2	Region 3	Region 4	Region 5	Region 6	Region 7	Region 8	Region 9	Region 10
Strongly Agree	0	1	3	3	1	2	3	0	2	2	2
Agree	0	2	3	3	4	5	3	2	0	9	6
Somewhat Agree	1	0	1	3	4	4	4	0	1	3	0
Somewhat Disagree	0	0	0	0	0	1	0	1	0	0	1
Disagree	0	0	0	0	2	0	1	0	0	1	1
Strongly Disagree	0	0	0	0	1	0	0	0	0	0	0

Figure 46. Composite percentages of Figure 45.

This perhaps indicates a programmatic gap between the mitigation and protection mission spaces. As indicated by the survey response data, the broad recognition and utilization of national doctrine with the real or perceived need for additional programmatic and organizational resources could be described as the makings of a "national doctrine echo chamber"—a condition wherein national thinking and operational posture has outpaced the development of the same thinking and operational posture at the state or local government level. In the context of state sovereignty and national supremacy, the strategic thinking and national doctrine exists, but the consistent and mature tactical organizations and programmatic resources within SLTT governments to adequately and/or evenly implement the national doctrine does not. This could also indicate that currently there is a strategic or tactical level programmatic "tragedy of the commons," or it may be emerging. In this condition, no one beyond an asset owner/operator has a clear and consistent feeling of ownership of the protection mission space. Therefore, significant tactical investment has not been made to develop and/or sustain this program mission space and, by extension, not maturing CIP as a discrete professional discipline. This was identified by some respondents in the open narrative question at the end of the survey, Table 1: Question 48 (N=52) where respondents were asked to provide one insight, effort, initiative, or idea to improve their CIP program. Of the 52 respondents to this question, six respondents (11.53 percent) proactively and specifically cited the need for more executive will and/or a stronger mandate from their executive leadership.

D. SURVEY SECTION: PERCEPTIONS AND VIEWS OF OPERATIONAL BUSINESS PROCESS

This block of questions centered on the respondents' general perceptions and views of the operational aspects of the critical infrastructure protection (security and resilience) enterprise. From an operational perspective, Figure 47 indicates that respondents felt very positive that their jurisdictions employed a method to identify critical infrastructure at risk (Question 33: Average 4.39, N=83) and also felt operationally very positive (Figure 48) that their jurisdiction

conducted sector and/or site-specific risk assessments that include threat, vulnerability, and consequence components (Question 34: Average 4.45, N=83). Cross-analysis of supporting data by jurisdiction type and federal FEMA region (see Figures 47A–47D in Appendix C) indicates generally consistent responses. Respondents were generally more positive than negative (as indicated in Figure 41) that their CIP staff members are appropriately trained (Question 26: Average 4.05, N=85). Additionally, as shown in Figure 50, respondents were generally more positive than negative that their CIP program maintained sector relationships through established liaisons/relationship managers (Question 31: Average 4.25, N=84). Finally, as illustrated in Figure 51, respondents were generally more positive than negative that their CIP program maintained sector relationships with sector working groups or coordinating councils (Question 35: Average 4.28, N=82).

The response data in Figure 51 was inversely supported by the response data represented in Figure 52 (Question 36: N=80), where respondents were asked to indicate more objectively with only “yes,” “no,” or “I don’t know” response options whether their jurisdiction maintained an engagement model with infrastructure owners and operators different from sector working groups or coordinating councils. As indicated in Figure 52, 47 respondents (58.75 percent) answered “no.” Of note, 15 respondents (18.75 percent) indicated, “I don’t know.” Respondents indicated at least occasional (to frequent) meetings between their jurisdiction’s CIP program and infrastructure owners and operators (Question 37: Average 4.14, N=81). Cross-analysis by jurisdiction type showed generally consistent responses, and there is some variation among the federal FEMA regions. Cross-analysis of supporting data (Figures 47–51) paints a generally positive operational picture.

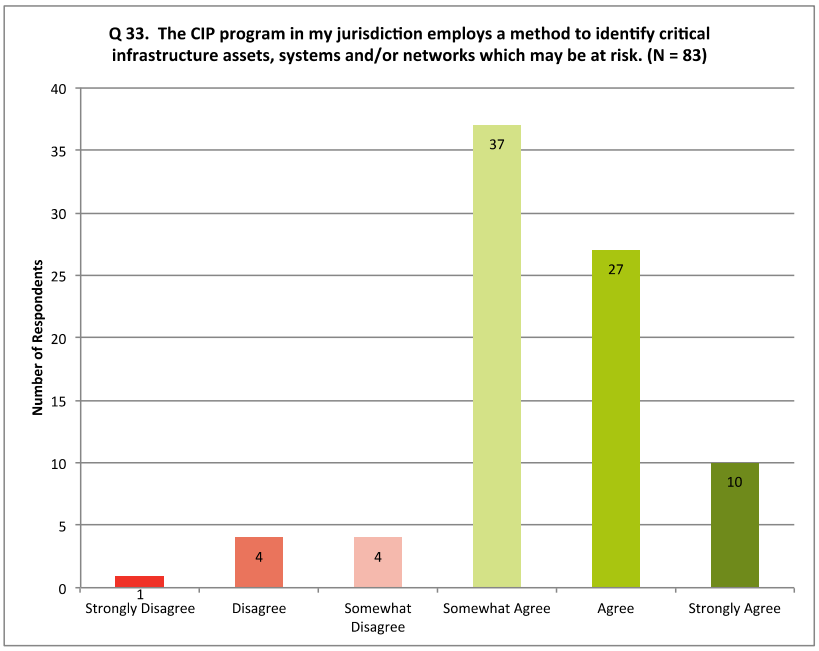


Figure 47. Respondents' perception on whether the CIP program in their jurisdiction employs a method to identify critical infrastructure assets, systems and/or networks that may be at risk.

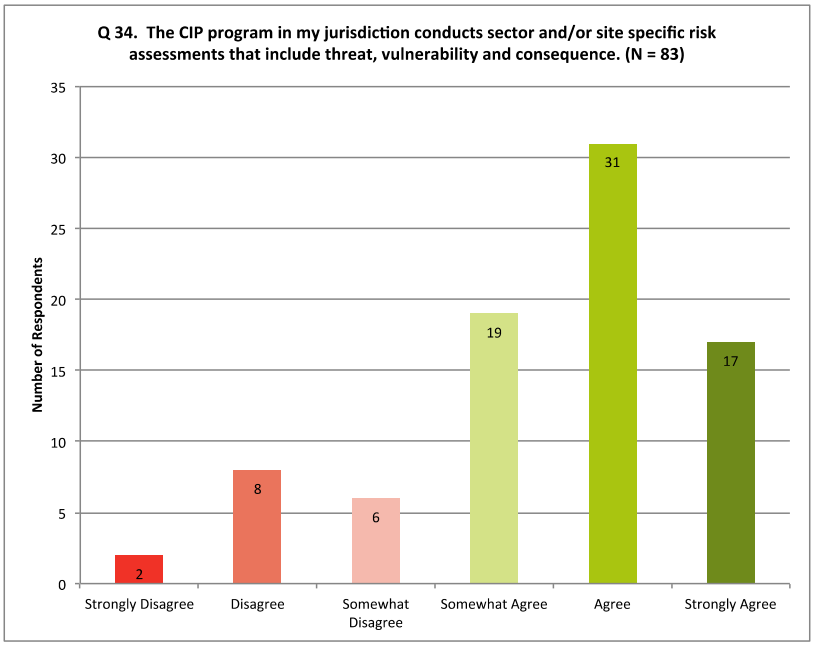


Figure 48. Respondents' perspective on whether the CIP program in their jurisdiction conducts sector or site specific risk assessments.

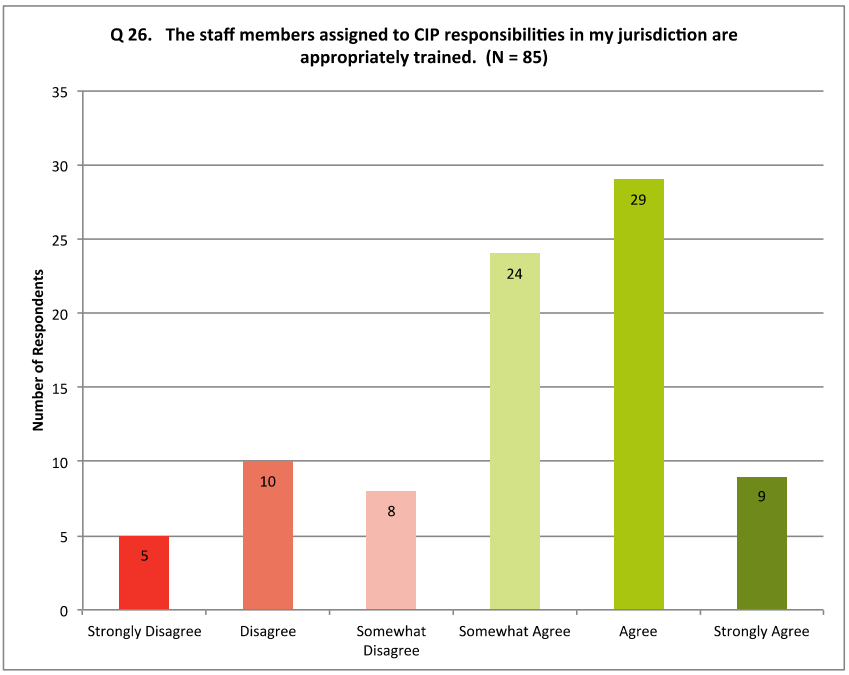


Figure 49. Respondents' perspective on whether staff assigned to CIP responsibilities in their jurisdiction are appropriately trained.

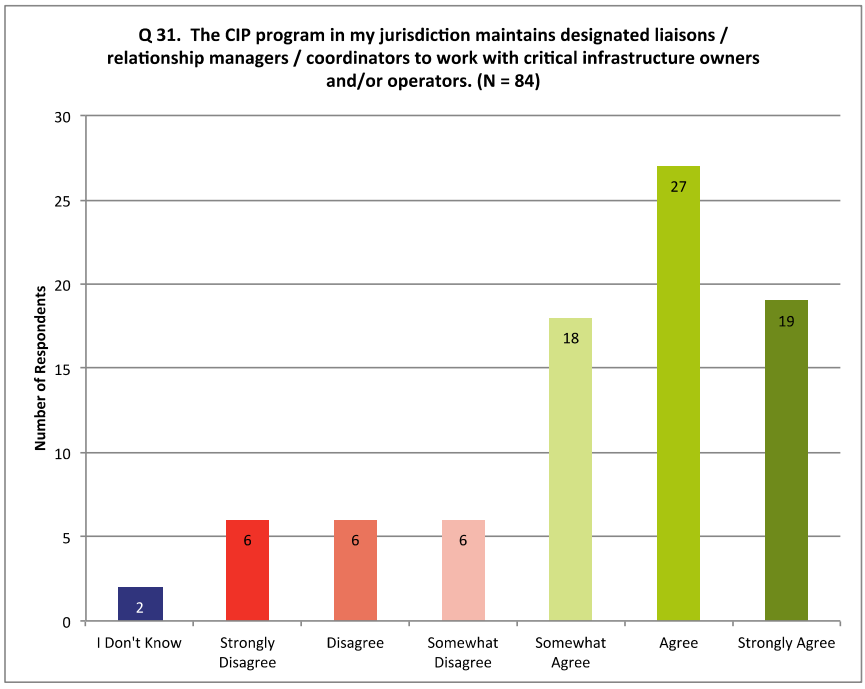


Figure 50. Respondents' perspective on whether the CIP program in their jurisdiction maintains designated liaisons / relationship managers / coordinators to work with critical infrastructure owners / operators.

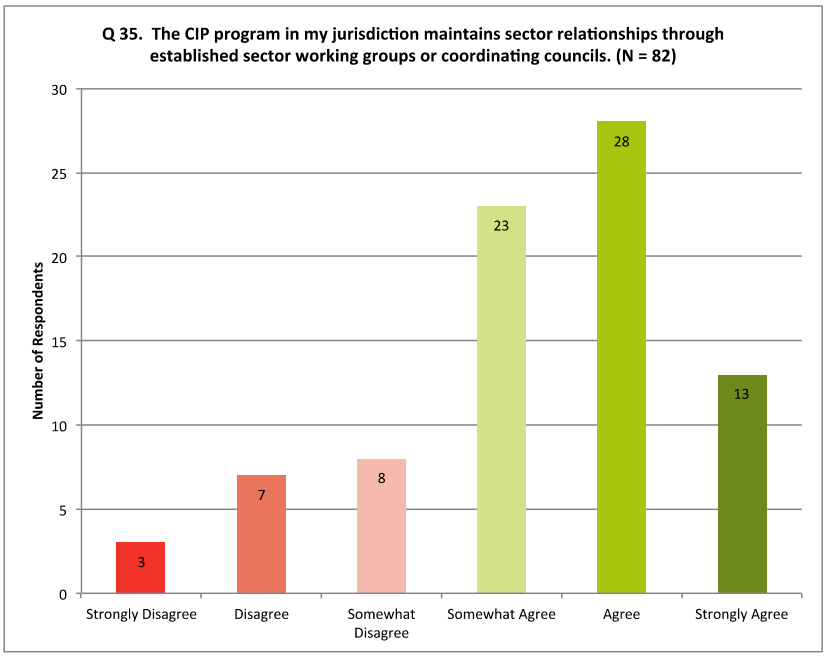


Figure 51. Respondents' perspective on whether the CIP program in their jurisdiction maintains sector relationships through established sector working groups or coordinating councils.

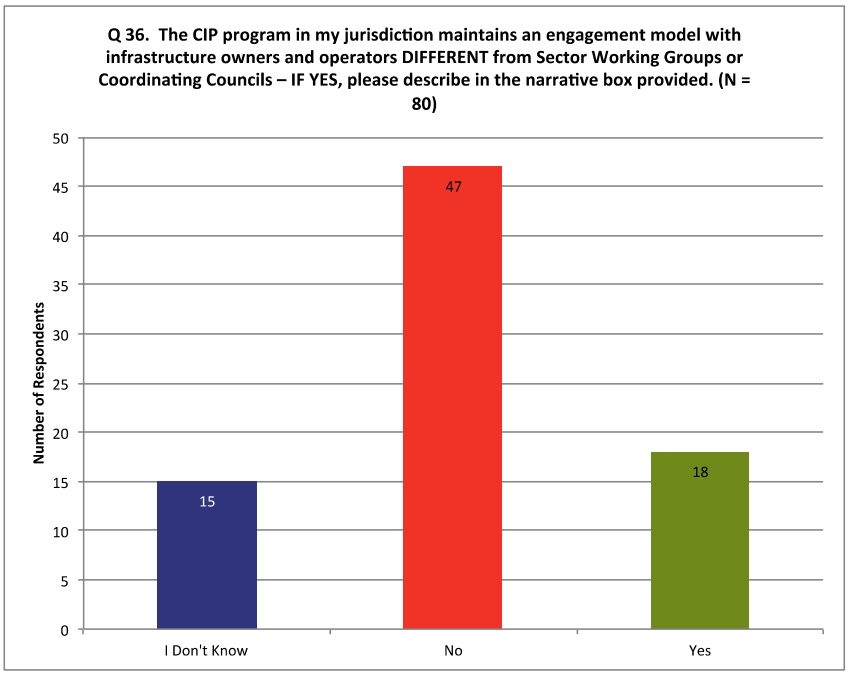


Figure 52. Respondents' knowledge on whether an infrastructure owner and operators engagement model different from sector working groups or sector coordinating councils is maintained in their jurisdiction.

Figure 53 indicates that almost all respondents (88 of 91 respondents (96.70 percent)) agreed, and over half of all respondents (56 of 91 (61.53 percent)) strongly agreed that there are many infrastructure assets, facilities, systems, and/or networks in their jurisdiction that requires all-hazard protection (security and resilience) (Question 16: Average 5.46, N=91). Cross analysis of support data (see Figures 53A–53J in Appendix C) by CIP practitioner/partner status, organization type, years of experience, jurisdiction type, and federal FEMA regions indicates that this thinking appears to transcend all disciplines, years of experience, level of government, and federal FEMA regions across the nation.

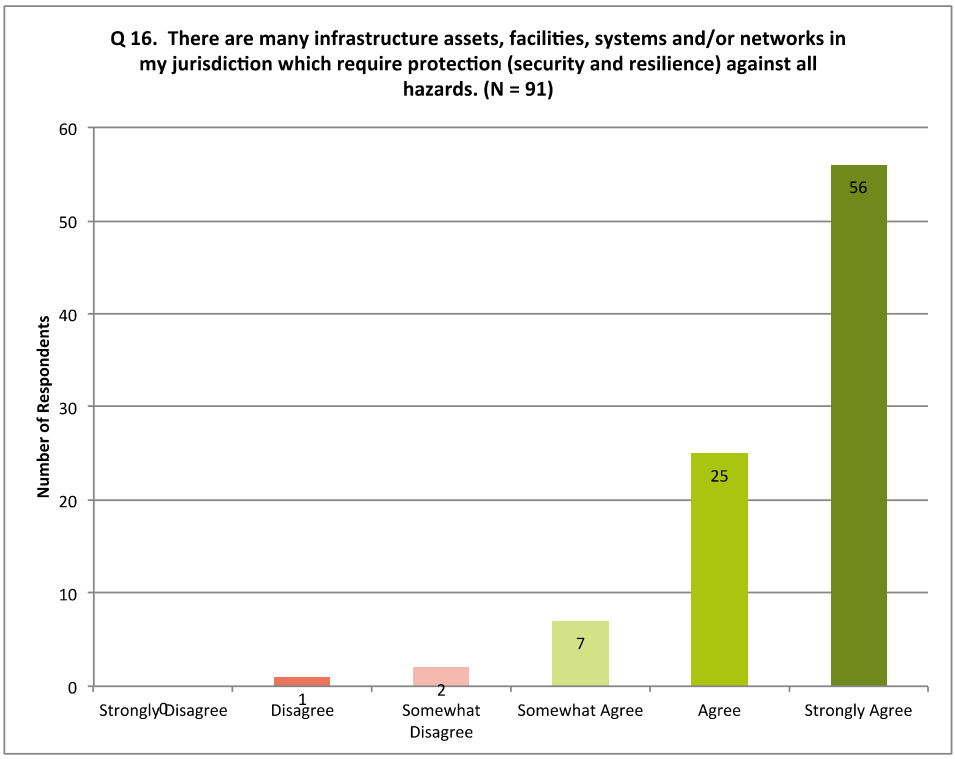


Figure 53. Respondents' perspective on whether there are many infrastructure assets in their jurisdiction that require all hazard protection.

When asked how much of the critical infrastructure in their jurisdiction is publicly owned or operated, respondent estimates (shown in Figure 54) generally

ranged evenly and the average of response given was 43 percent (Question 18: Average 43%, N=85). However, as depicted in Figure 54, a data cluster in the 15 to 25 percent estimate range was very distinct. Interestingly, these respondent estimates appear to roughly and inversely correlate to the widely known 85 percent statistic that is often cited as the percentage of critical infrastructure owned or operated by the private sector. Furthermore, as indicated in Figure 55, most respondents in this cluster indicated one to 10 years of experience as a CIP practitioner or partner—since the contemporary framing of CIP in 2001. It should be noted, that no literature was found during the literature review process that supported or substantiated the 85 percent statistic in any way.

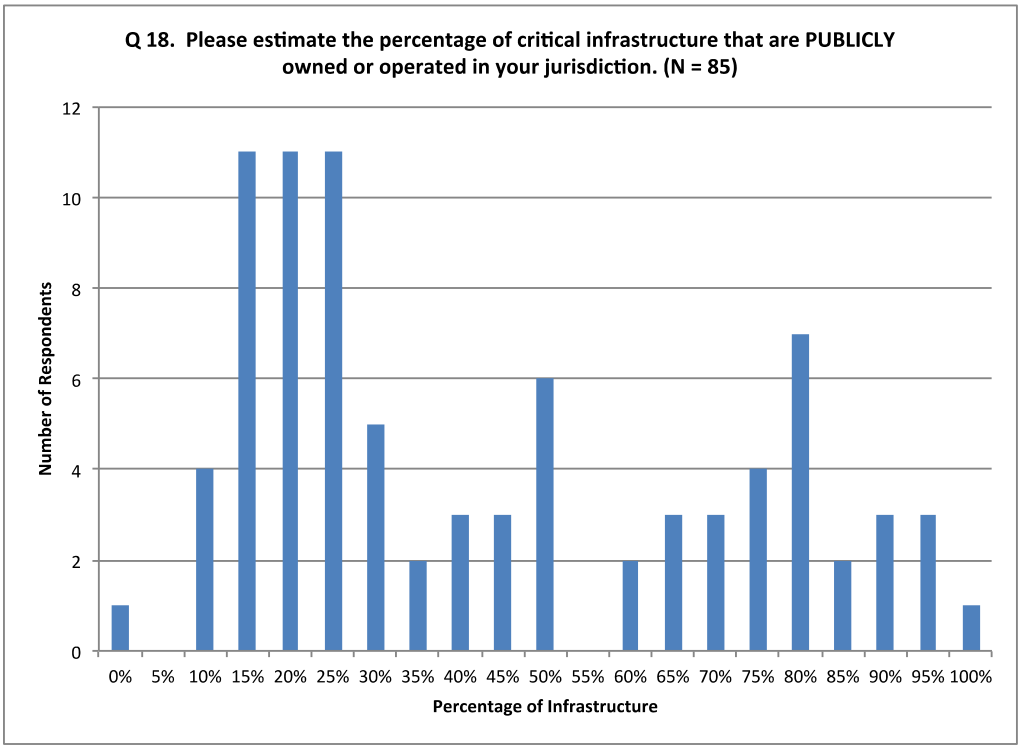


Figure 54. Respondents' estimate of the percentage of critical infrastructure in their jurisdiction that are publicly owned or operated.

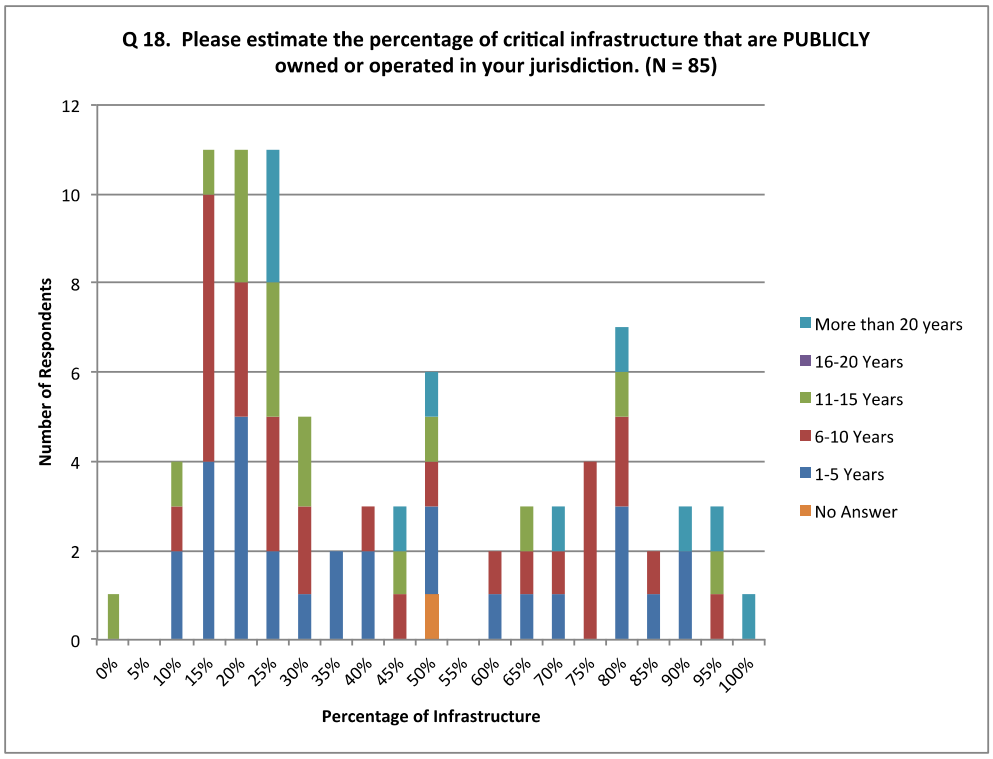


Figure 55. Respondents' estimate of the percentage of critical infrastructure in their jurisdiction that are publicly owned or operated cross-analyzed by years of experience.

Respondents also generally indicated positively that information sharing in both directions (Figures 56 and 57) between their CIP program and infrastructure owners and operators was occurring (Question 41: Average 4.37, N=82 and Question 42: Average 4.09, N=82). Respondents appear to generally feel that there is slightly more information being shared by CIP jurisdictional programs than the infrastructure owners and operators in their jurisdiction. Cross-analysis of support data (see Figures 56A–56F and Figures 57A–57F in Appendix C) by CIP practitioner/partner status, organization type, and jurisdiction type appear to be generally consistent in their responses. CIP partners tended to disagree at a notably higher rate of 30 percent (versus 15 percent for CIP practitioners) and 45 percent (versus almost 20 percent for CIP practitioners) respectively.

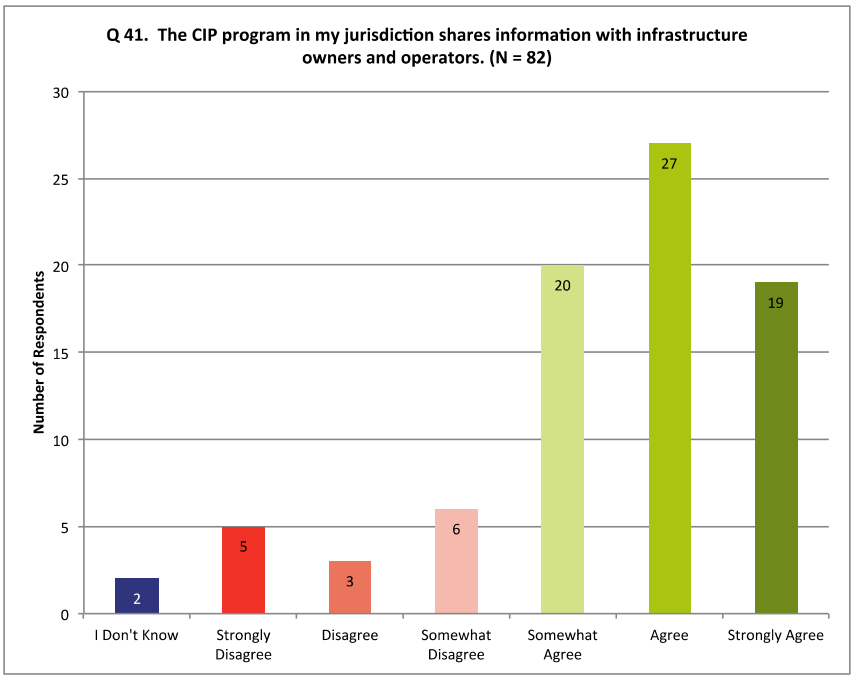


Figure 56. Respondents' perspective on whether the CIP program in their jurisdiction shares information with infrastructure owners and operators.

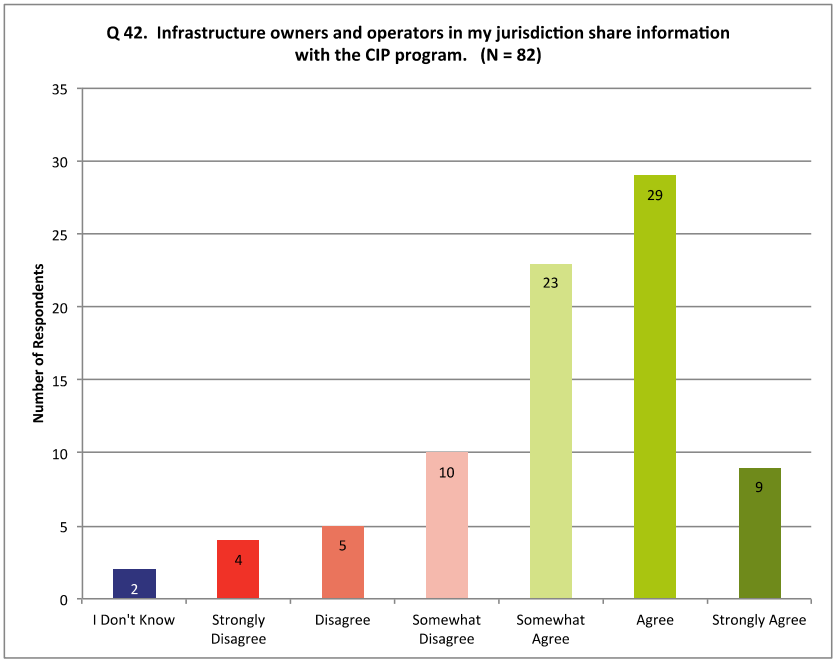


Figure 57. Respondents' perspective on whether infrastructure owners and operators in their jurisdiction share information with the CIP program.

As indicated by Figure 58, respondents solidly indicated a neutral to positive expression that their jurisdiction had shifted focus from critical infrastructure "protection" or "security" also including critical infrastructure "resilience" (Question 47: Average 4.00, N=81). It should be noted that almost half (43.20 percent) of respondents somewhat agreed that this shift has occurred. As further indicated by Figure 59, FEMA Region 4 had the highest rate of disagreement and Regions 8, 10, and 6 had the sharpest divide on respondents thinking.

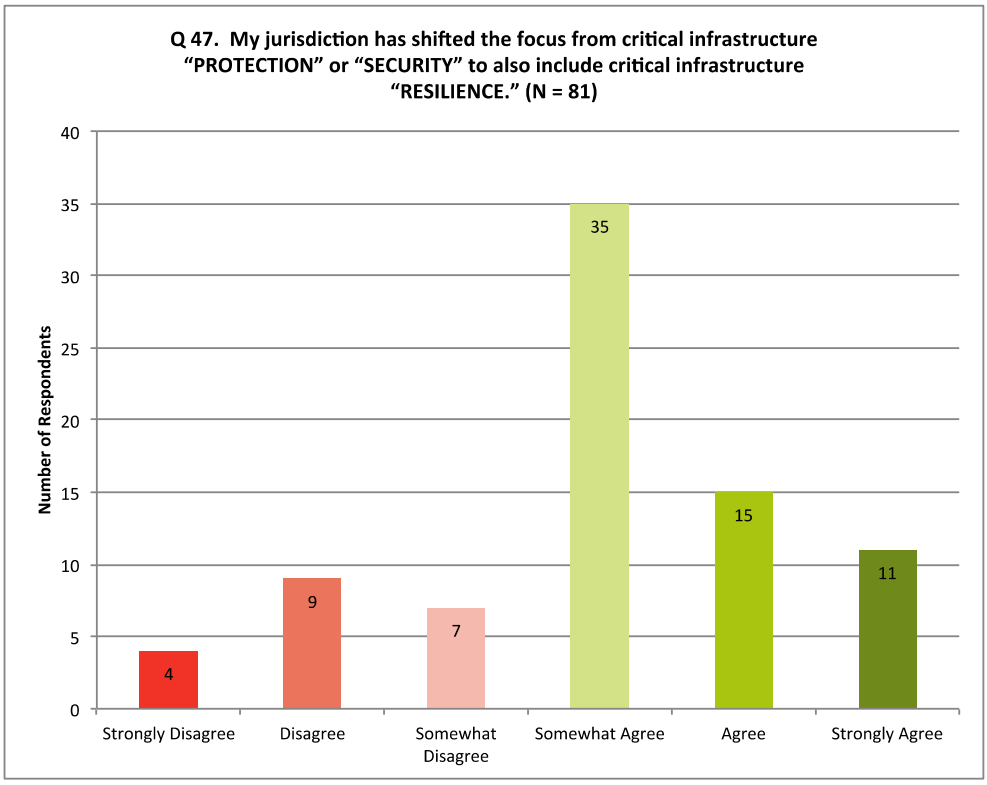
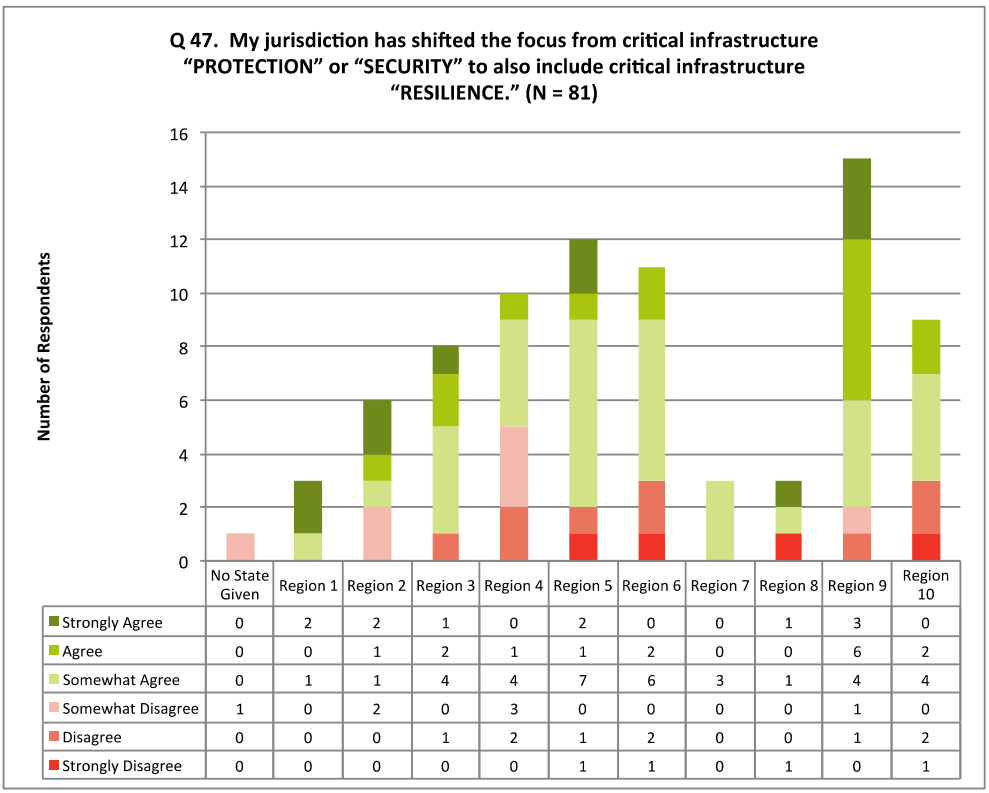


Figure 58. Respondents' perspective on whether their jurisdiction has shifted focus from critical infrastructure "protection" or "security" to also including "resilience."



	No State Given	Region 1	Region 2	Region 3	Region 4	Region 5	Region 6	Region 7	Region 8	Region 9	Region 10
Strongly Agree	0	2	2	1	0	2	0	0	1	3	0
Agree	0	0	1	2	1	1	2	0	0	6	2
Somewhat Agree	0	1	1	4	4	7	6	3	1	4	4
Somewhat Disagree	1	0	2	0	3	0	0	0	0	1	0
Disagree	0	0	0	1	2	1	2	0	0	1	2
Strongly Disagree	0	0	0	0	0	1	1	0	1	0	1

Figure 59. Respondents' perspective on whether their jurisdiction has shifted focus from critical infrastructure "protection" or "security" to also include "resilience" cross-analyzed by FEMA region.

E. SURVEY SECTION: RECOMMENDATIONS

The last question of the survey was an open-ended narrative opportunity for respondents to provide their views or judgment on what could be done in their jurisdiction to improve the critical infrastructure protection (security and resilience) program. Specifically, respondents were asked to provide one thing that could be done in their jurisdiction to improve their CIP program. A total of 52 respondents provided their views; many respondents provided more than one thing that could be done to improve their jurisdiction's program. Of interest, most of the respondent's suggested program enhancements centered on the five common themes. These themes were the need for additional or dedicated staffing; improved interaction, coordination, and information sharing with owners and operators, jurisdictional stakeholders and across the enterprise; additional or

dedicated program funding; the need for additional program resources or capability (not specifically citing staffing or funding); and the need for more executive will and/or a stronger mandate from their executive leadership.

The need for additional and/or dedicated CIP program funding was reinforced by many respondents in the open narrative question at the end of the survey. As indicated in Table 1, approximately one-third of respondents (16 of 52 respondents (30.77 percent)) identified the specific need for dedicated or additional staffing to create or increase program capacity (Question 48: N=52). Several respondents (12 of 52 respondents (23.08 percent)) suggested that improved interaction, information sharing, and coordination with asset owners or operators, jurisdictional stakeholders, and across the CIP enterprise was needed. Almost as many respondents (11 of the 52 respondents (21.15 percent)) specifically cited the need for more and/or dedicated CIP program funding. Beyond the call for additional or dedicated staffing and funding, the need for additional or dedicated program resources to create or expand program capability was also identified as a respondent theme. Eight of the 52 respondents (15.38 percent) identified the generic need for dedicated “resources” to expand or create a jurisdictional program, and some respondents included specific resource needs such as cyber, forecasting, planning, training, and assessments. Six of the 52 respondents (11.53 percent) proactively and specifically cited the need for more executive will and/or a stronger mandate from their executive leadership in order to enhance their jurisdiction’s program. Specifically noted by two respondents of the 52 respondents (3.85 percent), was the call to expand the DHS protective security advisor (PSA) and the cyber security advisor (CSA) programs as well as a need for a more integrated working relationship with the PSA assigned to their jurisdiction. One respondent suggested the need for public partners to integrate private partners and their representative associations into government response and recovery operations. Another respondent suggested that public CIP partners need to step aside and allow “private industry [to] take care of their own assets, [in the end] it will be more effective, cheaper, and

SAFER!" Table 1 includes all responses to Question 48 exactly as they were submitted.

Table 1. Question 48 Responses: "If there was one thing that could be done in your jurisdiction to improve the CIP program, what would that be?" (N=52)

Understand and create one.
More forecasting and planning
Funding to increase staffing as well as enhance salaries of current employees to encourage retention of experienced team members.
expand
Increased federal funding to support this effort.
Develop a stronger cyber capability
Dedicate full time staff to achieve the goals and objectives of the CIP mission. Staffing and a budget for target hardening would help our jurisdiction.
More interaction and communication between the stakeholders - more frequent meetings or discussions.
Improve program support though funding and personnel. This would allow for greater all-hazard analysis to support risk management decision making, enhanced information sharing, and stronger coordination.
Dedicate more staff time to the program.
Currently assigned duty of the regional fusion center
Cross sector meetings
More PSAs & CSAs
More of a unified and seamless working relationship with the DHS Protective Security Advisor. A lot of times, we seem to be at odds over what we are doing versus what they are doing.
More outreach to smaller privately own infrastructure and to address cyber across all sectors.
More staff and better guidelines from the state on what constitutes CIKR.
Full time CIP Program Manager
Federal Port Security Grant Program to provide funding support for Preventive Maintenance, Maintenance and Life Cycle Support for approved Security Infrastructure Risk Assessment Programs.
Better coordination of the many moving parts in the port security environment. Improve lines of communication and intelligence sharing among qualified port partners.
The entire premise of CIP has created an overlap between fusion centers, homeland security, and emergency management that is confusing to the public and government agencies. As CIP Units try to define themselves, scope creep sets in and they re-create programs that already exist through other disciplines. The CIP philosophy needs to be

re-thought from the "Is this really law enforcement's job" perspective?
Funding
Have City leadership/city council understand the urgency of needing a CIP program and keeping it optimally maintained.
Take the emergency management and homeland security functions out of the military department and place them under the governor's office, so that emergency management and homeland security become actual priorities in our state.
More staff as job expands one person shows make it hard.
staffing for public outreach
Provide a clear mandate from State and Federal entities, including funding.
Private industry does not trust CIP government based on what they do and not what they say. Government actions create a big mess, they walk away and private industry has to clean it up with limited time, resources and money. Let private industry take care of their own assets it will be more effective, cheaper and SAFER!
Bring back the Urban Area Security Initiative (UASI) program. That was a vital part of providing funding. Individual local agencies can't afford to provide the funding needed to carry out a quality program.
As always, funding for staff and implementation of goals & objectives.
More formal CIP programs, regional programs overlapping (complimentary), better staffed, more training available for entry level, professional development, and advanced CIP concepts.
Improved coordination/information sharing between CIP managers and Emergency Management. Taking the necessary steps to move beyond protection/prevention and towards resilience.
Reinvigorate the state's CIP program through increased awareness and outreach, staffing, knowledgeable leadership, and funding.
Have dedicated paid staff, not staff that do this as a added duty.
Formalize the program and allocate dedicated resources to it.
Assessments
The most important accomplishment would be coordinating fusion center activities, CIP activities, grant activities, HIRA/THIRA activities, and Federal outreach programs within our community under a single CIP Program. That is not any of the entities alone.
Provide for a CIP position to take responsibility for CIP planning, coordination and liaison.
Increase frequency of operational level interaction between protective personnel, who are not regularly assigned to CIP duties, and critical infrastructure partners.
communication
more education to the public on the value of having a relationship with CIP. Consistent message on what it is on a national level.
Dedicated funding w/in the HSGP to support additional staff that could expand the network of services DHSES provides. This includes direct assistance to state agencies and authorities, local governments and private sector partners in all aspects of critical

infrastructure and resilience planning. Given current resource constraints our capacity cannot keep up with our capabilities and demand.
More training to provide vulnerability assessments
I am a one man "division" with no admin. assistance. A good deal of my time is taken up by fusion center activities, primarily Homeland Security, but this limits the time available for IN PERSON outreach. I do connect with most sectors on a semi regular basis via email -
Better maintain an up-to-date active roster of all CIKR assets, along with points-of-contact.
Educate the politicians on how important the CIP program is and why their support is needed to have a more effective program.
increased staffing not dependent on grant funding mandatory requirements to comply/participate in program for private industry
have dedicated staff to look at all components of the risk
Additional Manpower.
State funding
Dedicated trained staff and liaison personnel
Begin pulling our private sector CIKR partners into response and recovery using their respective associations like the Water Association Resource Network, giving them visibility on our Webeoc to inform our actions, and vice versa. Something along the lines of a business EOC, only get them into earlier stages of planning and training too. Already happening in some county\local jurisdictions. But is becoming severely strained with the loss of ACAMS as far as being able to standardize and compare protective measures, and share info between public an private partners.
1. Executive leadership approve and implement the DRAFT State Homeland Security Framework that is currently under internal executive review. 2. Executive leadership approve and implement the DRAFT State Critical Infrastructure Protection and Resiliency Strategy that is currently under executive review.

V. SUMMARY OF KEY FINDINGS

The survey conducted for this thesis captured a lot of rich data and respondent perspective on the current state of the critical infrastructure protection (security and resilience) mission space within SLTT jurisdictions. Some of the key findings identified in this data are summarized here (Table 2). Strategically, most respondents clearly felt that their jurisdictions do recognize and utilize the concepts outlined in the *National Infrastructure Protection Plan* (Question 12: Average 4.92, N=90). Furthermore, most respondents also indicated positively that CIP has become or should become and be maintained as a discrete professional discipline (Question 9: Average 4.18, N=90 and Question 10: Average 4.91, N=91).

Table 2. Summary of key findings

There is a lack of dedicated and consistent CIP (security and resilience) program funding.
There is a lack of dedicated and mature tactical CIP (security and resilience) organizations at or within the SLTT levels of government.
There is a lack of dedicated and consistent CIP (security and resilience) program staffing.
There is significant variation in the consistency and local adaptation with which the CIP (security and resilience) mission is interpreted, understood, applied and implemented across the nation.

As indicated in Figure 9, many respondents indicated that their jurisdictions have invested their own operational funds to support the staffing of their critical infrastructure protection program (37.5 percent of program staff salary is supported by operational budgets). As further indicated in Figure 9, it also appears that the financial investments in CIP staff are significantly dependent on federal grant funds (55.8 percent of program staff salary is supported by federal financial grants).

The three most common types of federal grant funds invested in program staffing were the HSGP, UASI, and EMPG. Of note, the utilization percentages of the funding sources indicated (Figures 9–11) do not change significantly when filtered by 80 percent plus utilization of a single funding source indicating a dependence on these federal funding mechanisms. The utilization of federal grant funds increases when cross-analyzed against CIP staff members where staff members are not fully dedicated to CIP program responsibilities. Figure 12 indicates a 65.6 percent utilization of federal financial grants in this instance. The high utilization of federal grant funds to support staff members not fully dedicate to CIP responsibilities indicates both a critical dependence on these federal funds and inherent programmatic vulnerability.

Though analysis of respondent data indicates an all inclusive jurisdictional average of 4.9 fulltime and 4.3 part-time staff members assigned to CIP responsibilities, over half the respondents (59.57 percent) indicated that where there is fulltime CIP programmatic staffing within a state or local governmental jurisdiction, it appears to be one or two fulltime staff members. When directly asked whether the CIP program or organization in their jurisdiction was adequately staffed, most respondents were overwhelmingly negative, though there was a pocket of positive respondents. Based on respondent data, current staffing levels appear to be inadequate (Question 25: Average 2.62, N=86). This sentiment was very clearly indicated by the survey response data of multiple questions.

Most respondents did indicate that the CIP program staffs in their jurisdiction have a very strong productive working relationship with the U.S. Department of Homeland Security protective security advisor (PSA) assigned to their jurisdiction (Question 14: Average 4.93, N=91). This very strong productive working relationship is a very positive reflection of DHS and the PSA program and certainly indicates great collaboration between professionals across the levels of government; however based on provided staffing levels, this may

indicate a level of underlying programmatic dependence on the federal government and the PSA program to deliver local CIP programs.

It appears that the CIP tactical and operational mission and mandate are highly adapted locally[59] but are not as clearly and/or consistently interpreted, applied, implemented (Question 43: Average 3.12, N=83; Question 44: Average 3.55, N=83; and Question 45: Average 3.64, N=83) or understood (Question 38: Average 3.61, N=83 and Question 39: Average 3.59, N=82) within jurisdictions across the nation. Operational CIP program responsibilities in state and local government appear to be managed as a component function (Question 30: Average 3.93, N=84) with generally minimal programmatic staffing. Respondents generally disagreed when asked if their jurisdiction's CIP program was managed by an organizational component entirely dedicated to CIP as its core mission (Question 29: Average 2.95, N=85). The data indicates a clear lack of dedicated CIP organizations at or within the state and local levels. A large majority of respondents felt significantly positive that the CIP/risk management mission should be more closely aligned to the mitigation and preparedness mission space of emergency management offices and agencies (Question 20: Average 4.69, N=86).

Most respondents were generally neutral on whether the CIP mission and organization in their jurisdiction are well understood by stakeholders (Question 38: Average 3.61, N=83 and Question 39: Average 3.59, N=82). This neutral view of respondents indicating a lack of mission and organizational clarity by stakeholders may indicate a lack of clear role or mandate or the ability to communicate effectively the role or mandate. The lack of stronger understanding by stakeholders may hinder cooperation or retard coordination among partners. The expressed lack of mission and organizational clarity noted might also be impeding mission implementation or fostering a generally neutral perception regarding CIP mission implementation that was clearly seen in the response

[59] Sagarin, "Natural Security for a Variable and Risk-Filled World," 6–8.

data. Though the job appears to be getting done operationally, from a tactical organizational perspective, most respondents were generally neutral to negative about whether the CIP mission was fully implemented, implemented well, and well managed (Question 43: Average 3.12, N=83; Question 44: Average 3.55, N=83; and Question 45: Average 3.64, N=83) in their jurisdiction. A solid neutral to positive respondent expression was noted; respondents' jurisdictions had shifted focus from critical infrastructure "protection" or "security," also including critical infrastructure "resilience" (Question 47: Average 4.00, N=81).

Overall, the strategic national doctrine, SLTT strategic plans (Question 13: N=91), and operational concepts and tools appear to be well recognized and utilized. Moreover, there seems to be a reality or perception that the bridging tactical component between strategy and operations has not been fully developed or realized—a noted lack of consistent, dedicated, and mature tactical organizations, business process (including goals and objectives) (Question 15: Average 3.52, N=91 and Question 40: Average 3.57, N=82), staff, and sustained programmatic resources and funding was a clear theme throughout the analysis of participant's responses.

VI. RECOMMENDATIONS

The key issues identified by this research present a great opportunity to improve the ways in which we pursue the national critical infrastructure security and resilience mission. Three specific opportunities were identified: (1) sustained and dedicated funding; (2) organizational development and alignment; and (3) an integrated national approach with regional constructs.

A. FUNDING

Access and availability of financial resources is a cornerstone of any successful program or endeavor. There are many traditional and innovative ways to fund, support, or sustain a local public program or initiative. A few examples include local operating budget supported by local taxes, a fee based system, financial bonding, individual, or corporate donations. To date and in general terms, it appears that the direct investment of SLTT dollars to develop and/or sustain SLTT tactical organizations exists but has been modest. SLTT investment of federal HSGP funding was noted, as well as several other federal grant funding streams that have been congressionally authorized and appropriated to provide SLTT organizations funding for specific risk-based security efforts. These include the Port Security Grant Program (PSGP),[60] the Transit Security Grant Program (TSGP),[61] and the Buffer Zone Protection Program (BZPP).[62]

---

[60] Federal Emergency Management Agency, *U.S. Department of Homeland Security Funding Opportunity Announcement (FOA) FY 2014 Port Security Grant Program (PSGP)* (Washington, DC: Federal Emergency Management Agency, 2014), http://www.fema.gov/media-library-data/1396623742630-9e497a99bef3e3c0265bbf84993b5e69/FY_2014_PSGP_FOA_Final_Revised.pdf.

[61] Ibid.

[62] Federal Emergency Management Agency, *Fiscal Year 2010 Buffer Zone Protection Program: Guidance and Application Kit* (Washington, DC: Federal Emergency Management Agency, 2012), http://www.fema.gov/media-library-data/20130726-1750-25045-6174/fy_2010_bzpp_guidance_final.pdf.

Given the modest direct SLTT investment seen to date, the most realistic and expedient opportunity to systemically fund SLTT critical infrastructure security and resilience tactical organizations, programs, and operations may be through additional federal funding. Further availability of this sustained and targeted federal funding to SLTT critical infrastructure security and resilience organizations may be the most viable approach to ensure the most uniformed and even development and implementation of tactical organizations and programs across the nation because of the federal government's ability to craft new grant funding availabilities or to reshape the priorities and application of existing and currently available grant funds.

There may be additional opportunities to provide systemic federal financial assistance to support SLTT tactical organization, program and operations development, implementation, and sustainment. For its part, Congress could further appropriate a new definitive programmatic line of funding to support state and local government critical infrastructure security and resilience organizations, programs, and their associated operational activities. Similar in approach to the Emergency Management Grant Program (EMPG),[63] which provides support to state and local emergency management organizations to create and sustain a system of emergency preparedness to protect life and property, Congress could create a discrete Critical Infrastructure Resiliency Grant Program (CIRGP) to support organizational development, sustain dedicated CIRGP staff, and associated programmatic and operational activities. Additionally, Congress has directed a 25 percent pass through requirement to law enforcement to support terrorism prevention activities known as the *Consolidation of Law Enforcement Terrorism Prevention Activities* (LETPA).[64] The LETPA requirement can be

[63] Federal Emergency Management Agency, *Funding Opportunity Announcement: FY 2014 Emergency Management Performance Grant* (Washington, DC: Federal Emergency Management Agency, 2014), http://www.fema.gov/media-library-data/1398433298042-f8d5c17604fdb97c5ef5b49419a7cf01/FY2014_EMPG_FOA_Revised_508.pdf, 3.

[64] Federal Emergency Management Agency, *Funding Opportunity Announcement (FOA) FY 2014 Homeland Security Grant Program (HSGP)* (Washington, DC: Federal Emergency Management Agency, 2014), http://www.fema.gov/media-library-data/1395161200285-5b07ed0456056217175fbdee28d2b06e/FY_2014_HSGP_FOA_Final.pdf, 11.

fulfilled with funds from the State Homeland Security Program (HSGP), the Urban Area Security Initiative (UASI), or a combination of both.[65] Under this already existing pass through requirement, eligible funding activities include those outlined in the *National Prevention Framework*[66] and the *National Protection Framework*.[67] Certainly, operations and activities supported under the *National Prevention Framework* enhance the security of our nations critical infrastructure; however, it appears this provision is generally under-recognized or underutilized as a systemic programmatic funding mechanism to support state and local government protection and resilience operations and activities. Additional education and awareness (in the form of funding workshops, bulletins or otherwise) of these funding provisions within the critical infrastructure security and resilience community is recommended. It is possible that the current funding requirements in the prevention mission space fully obligates these funds on a jurisdictional basis thereby creating contention for these resources.

Another option is at the policy level, the DHS or FEMA could prioritize this funding through grant guidance and requirements. Similar in spirit and intent to the congressional LETPA funding mandate, the DHS or FEMA could create a discrete protection mission policy mandate whereby a percentage of existing HSGP or EMPG funds could be directed to support systemic critical infrastructure security and/or resilience activities and the requisite program and organizational development as outlined in the *National Infrastructure Protection Plan* and the *National Protection Framework*.[68]

---

[65] Ibid., 11, 29–30, 40.

[66] U.S. Department of Homeland Security, *National Prevention Framework* (Washington, DC: U.S. Department of Homeland Security, 2013), http://www.fema.gov/media-library-data/20130726-1913-25045-6071/final_national_prevention_framework_20130501.pdf.

[67] U.S. Department of Homeland Security, *National Protection Framework*, 1st ed. (Washington, DC: U.S. Department of Homeland Security, 2014), http://www.fema.gov/media-library-data/1406717583765-996837bf788e20e977eb5079f4174240/FINAL_National_Protection_Framework_20140729.pdf.

[68] Federal Emergency Management Agency, *FOA FY 2014 Homeland Security Grant Program*, 52.

Table 3. Summary of key findings aligned to recommendations: Funding (A).

FINDING	A. Funding	B. Alignment	C. HSIB
There is a lack of dedicated and consistent CIP (security and resilience) program funding.	X		
There is a lack of dedicated and mature tactical CIP (security and resilience) organizations at or within the SLTT levels of government.	X		
There is a lack of dedicated and consistent CIP (security and resilience) program staffing.	X		
There is significant variation in the consistency and local adaptation with which the CIP (security and resilience) mission is interpreted, understood, applied and implemented across the nation.			

B. CLOSER ALIGNMENT TO EMERGENCY MANAGEMENT

Based on survey responses, closer and formalized organizational and/or programmatic alignment to the mitigation and preparedness mission space of emergency management should be explored.

The Commonwealth of Australia provides a model example of this close doctrinal alignment. With the 2009 publication of the Australian CIR strategy, the Commonwealth recognized a clear nexus between the resilience of critical infrastructure and emergency management. This includes an expanded emergency management mandate and portfolio to facilitate greater resiliency. This expanded emergency management mission space and portfolio is further defined and outlined in Australia's *National Strategy for Disaster Resilience* (NSDR) as published by the Council of Australian Governments (COAG) in February 2011.[69] The Australian disaster resilience strategy further builds upon

[69] Council of Australian Governments, *National Strategy for Disaster Resilience* (Barton, Australia: Council of Australian Governments, 2011), https://www.ag.gov.au/EmergencyManagement/Documents/NationalStrategyforDisasterResilience.pdf.

the whole-of-nation concept and the notion of shared responsibility in becoming a resilient nation. This shared responsibility includes business, community, and individuals as the cornerstones.

Since 2009, the interconnected Australian approach integrating critical infrastructure, business, and individual preparedness together is enhanced resilience—each with its own responsibility to build a resilient Australia. The common thread tying Australian critical infrastructure and emergency management together is resiliency. There is recognition in the Australian whole-of-nation approach that individual people are the individual threads that collectively comprise the fabric of a community—as a private resident, an employee or business-person—if the individual is more resilient, the community is more resilient and by extension the nation is more resilient.

Domestically, the White House and the U.S. Department of Homeland Security[70] first recognized this subtle shift in thinking from a "protection" to an all-hazard capabilities based, whole community "resilience" mindset of national preparedness with the publication of *Presidential Policy Directive 8: National Preparedness*.[71] The subsequent publication of *Presidential Policy Directive 21* (PPD 21)[72] and the 2013 *National Infrastructure Protection Plan* (NIPP 2013)[73] further defined the evolution of a strictly "protection" mindset to include "security" and "resilience." Additional definitional outlines are also contained within the national mission frameworks. From a doctrinal and organizational perspective, the United States appears to generally maintain critical infrastructure protection (security and resilience) and emergency management as two discrete (in some cases almost mutually exclusive) parallel workflows. Perhaps one of the only currently recognized operational touchpoint between critical infrastructure and

[70] Ibid., 32.

[71] White House, *Presidential Policy Directive/PPD-8: National Preparedness* (Washington, DC: White House, 2011), 4, 6.

[72] White House, *Presidential Policy Directive/PPD-21*.

[73] U.S. Department of Homeland Security, *NIPP 2013*.

emergency management enterprises is during the post-event recovery phase within which the two must (or should) collaborate to restore impacted infrastructure. This organizational separation may be very necessary, appropriate, and sustainable within the context of federal and state governments. Based on respondent data, it appears that the need or sustainability of discrete and/or parallel critical infrastructure and other public safety (i.e., law enforcement and emergency management) organizations softens with the more local levels of government. Respondent data indicates that local adaptation[74] of blended organizations and associated blended responsibilities appears to be currently prevalent.

Extending and applying Egli's resiliency roots logic,[75] the deeper, stronger, and more mature programmatic and organizational roots of the emergency management discipline may provide a stronger foundation for critical infrastructure protection (security and resilience) activities at more local levels of government. Although, in many instances emergency management organizations can be understaffed and/or under-resourced—based on respondent data—it appears that both critical infrastructure and emergency management partners across the state and local governments spectrum would embrace such an alignment. The more mature root system of the emergency management preparedness and mitigation space could serve critical infrastructure practitioners well in two ways.

First, organizational and/or programmatic alignment of the protection mission space with the preparedness and mitigation mission space (and the emergency management organization within which it resides) could allow for more effective application of the emergency management organizational structure and resources to operationally support the protection mission. Furthermore, leveraging established emergency management structures could allow protection practitioners to collaborate more efficiently across the whole

[74] Sagarin, "Natural Security for a Variable and Risk-Filled World," 6–8.

[75] Egli, *Beyond the Storms*, 30.

community to support steady-state protection activities.[76] Second, a closer alignment of these mission spaces could ensure that CIP (security and resilience) resource requirements and gaps are more adequately reflected in the *Threat Hazard Identification and Risk Assessment (THIRA)*,[77] as well as each states' *state preparedness report* (SPR).[78] This requisite planning and preparedness,[79] in turn, could make protection resource requirements better known and understood, as well as strengthen the alignment between critical infrastructure sectors, and the related emergency management emergency support function (ESF),[80] and recovery support function (RSF) to each. This could lead to further programmatic awareness of associated stakeholders, increased funding, and accelerated program development. Certainly, this close alignment is consistent with the *National Infrastructure Protection Plan* (NIPP) 2013.[81] As indicated by Figure 60, a clear and integrated continuum among the national mission areas is contemplated and expected.

[76] U.S. Department of Homeland Security, *National Protection Framework*, 22.

[77] Federal Emergency Management Agency, *FOA FY 2014 Homeland Security Grant Program*, 9;

Federal Emergency Management Agency, *Funding Opportunity Announcement: FY 2014 Emergency Management Performance Grant*, 5.

[78] Federal Emergency Management Agency, *FOA FY 2014 Homeland Security Grant Program*, 9.

[79] White House, *The National Strategy for The Physical Protection*, x.

[80] U.S. Department of Homeland Security, *NIPP Supplemental Tool: Connecting to the NICC and NCCIC* (Washington, DC: U.S. Department of Homeland Security, 2013), http://www.dhs.gov/sites/default/files/publications/NIPP-2013-Supplement-Connecting-to-the-NICC-and-NCCIC-508.pdf, 5–6.

[81] U.S. Department of Homeland Security, *NIPP 2013*, 32.

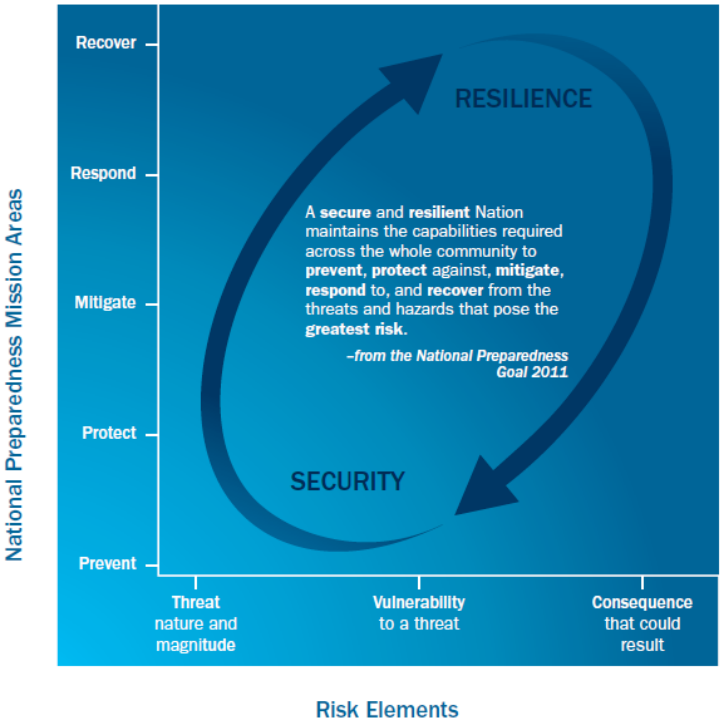


Figure 60. Critical infrastructure risk in the context of national preparedness[82]

Table 4. Summary of key findings aligned to recommendations: Alignment (B)

FINDING	A. Funding	**B. Alignment**	C. HSIB
There is a lack of dedicated and consistent CIP (security and resilience) program funding.	X		
There is a lack of dedicated and mature tactical CIP (security and resilience) organizations at or within the SLTT levels of government.	X	**X**	
There is a lack of dedicated and consistent CIP (security and resilience) program staffing.	X	**X**	
There is significant variation in the consistency and local adaptation with which the CIP (security and resilience) mission is interpreted, understood, applied and implemented across the nation.		**X**	

[82] Ibid., 19.

C. HOMELAND SECURITY INDUSTRIAL BASE

The survey results illustrated significant and rightful variation in the local adaptation, clarity and consistency with which the CIP (security and resilience) mission is interpreted, understood, applied, or implemented across the nation. One opportunity to even these variations would be through the creation of a nationally recognized Homeland Security Industrial Base (HSIB). The notion of critical modern industrial infrastructure, the beginnings of the modern defense industrial base,[83] and the need to protect it[84] can be traced back to the global tension and lead-up to World War I. The United States Industrial Alcohol (USIA) company distilled molasses into industrial grade alcohol, which was a key component to produce military munitions, including dynamite, smokeless powder, and high explosives.[85] In 1915, USIA was one of the largest producers of industrial alcohol in the United States and a critical supplier to the then Department of War and allied European governments.[86] The critical nature of USIA's Boston operation and the need to protect it was illustrated in April of 1917. In the context of a citywide threat warning issued by Boston's district attorney that bands of violent anarchists were targeting the city. To better protect its infrastructure and operations against sabotage, USIA hired guards who were sworn-in as special police officers to augment the single Boston police officer regularly posted to the USIA Boston operation.[87]

The concepts of further refined modern thinking of cornerstone infrastructure critical to our national interests dates back to the Defense Production Act of 1950 (DPA) that was passed to ensure prompt supply and

---

[83] Stephen Puleo, *Dark Tide: The Great Boston Molasses Flood of 1919* (Boston, MA: Beacon Press, 2004), 11, 16.

[84] Ibid., 59.

[85] Ibid., 11.

[86] Ibid., 9–11,16.

[87] Ibid., 58–59.

adequate quantities of needed military and civilian goods.[88] As prompted by then President Harry S. Truman, the infrastructure outlined in the DPA included agriculture, energy (all forms of energy), health, transportation (all forms of civil transportation), defense (in the context of water resources), and commerce.[89] President Barack Obama has more recently reinforced the critical nature of these same infrastructure sectors in the context of national defense needs.[90] By executive order, President Obama has directed federal executive departments and agencies not only to support all hazard plan and program development to meet military and civilian demand requirements but also to foster cooperation and "improve the efficiency and responsiveness of the domestic industrial base to support national defense."[91] He outlined the National Security Council, the Homeland Security Council, and the National Economic Council as the coordinating policy forum for this purpose.[92]

Implicit among the named DPA infrastructure is the dependency and interdependency that commerce and manufacturing have on what is now thought of in the civilian infrastructure protection community as *lifeline* infrastructure sectors. The foundational infrastructure on which all other sectors are dependent or *lifeline* critical infrastructure sectors are defined as the energy, water, transportation, communications,[93] and financial services[94] sectors.

---

[88] Daniel H. Else, *Defense Production Act: Purpose and Scope* (RS20587) (Washington, DC: Congressional Research Service, 2008), http://fas.org/sgp/crs/natsec/RS20587.pdf, 1.

[89] Chanl Wiggins, *Use of the Defense Production Act to Reduce Interruptions in Critical Infrastructure and Key Resource Operations During Emergencies: Fiscal Year 2009 Report to Congress* (Washington, DC: Federal Emergency Management Agency, 2009), 4.

[90] Exec Order No. 12919 (2012), §102, 201, http://www.whitehouse.gov/the-press-office/2012/03/16/executive-order-national-defense-resources-preparedness.

[91] Ibid., §103.

[92] Ibid., §104.

[93] Lau, and Scott, *Strengthening Regional Resilience*, 3, 13; Hardenbrook, "The Need for a Policy Framework," 1.

[94] Lau, and Scott, *Strengthening Regional Resilience*, 13; Egli, *Beyond the Storms*, 34.

The productive and collaborative benefit of regional constructs are encouraged by the National Governors' Association (NGA)[95] and have been recognized in many instances to include the Urban Areas Security Initiative (UASI) program, the UASI National Capitol Region, the New York-New Jersey Transportation Operations Coordinating Committee (TRANSCOM), and metropolitan planning organizations (MPO) as required under federal transportation law.[96] Further expanding upon or leveraging the successful transportation MPO model or the nature of the UASI model to include an emphasis on the lifeline infrastructure on which it depends should be examined.

The creation of a Homeland Security Industrial Base (HSIB), initially comprised of the defined lifeline infrastructure sectors, could bring a sharper programmatic focus to intra- and inter-regional critical infrastructure protection and resiliency (CIPR) activities generally and specifically within and among these infrastructure sectors and therefore should be explored and considered. In the context of the *National Protection Framework*,[97] the concept of a HSIB could be integrated with legacy DPA mandates and authorities. In addition, special expectations and preferential technical, analytical, contractual, or financial consideration could be required and afforded the sectors of a HSIB as they are currently under the DPA.[98] The integration of a HSIB with DPA mandates and authorities could also serve to eliminate or bridge much of the artificial distinctions that are currently found between military and civilian doctrine. Integrated national doctrine should result in sharpened national programmatic focus on a more finite scope of infrastructure sectors, which will allow the CIPR mission to be more clearly understood, programmatically consumable, and

---

[95] Carmen Ferro, David Henry, and Thomas MacLellan, *A Governor's Guide to Homeland Security* (Washington, DC: National Governor's Association, 2010), 33.

[96] U.S. Government Accountability Office, *Homeland Security: Effective Regional Coordination Can Enhance Emergency Preparedness* (GAO-04-1009) (Washington, DC: U.S. Government Accountability Office, 2004), http://www.gao.gov/assets/250/244172.pdf, 4–6, 20–23.

[97] U.S. Department of Homeland Security, *National Protection Framework*.

[98] Wiggins, *Use of the Defense Production Act*, 3–4.

facilitate a steady-state protection posture.[99] It would serve the needs of our national defense complex as well as the commercial and economic needs of state and local communities and therefore would serve to further strengthen the commercial and economic fabric of the nation and remain true to our federalist system.

As a macro analog to the Egli resiliency roots,[100] with a sharper focus, the analytical, protection, and resilience work necessary within and among each sector of the HSIB could be more directly supported and matured. Once established in a comprehensive manner, the dependencies and interdependencies among and between HSIB sectors could serve as a baseline tier (roots) for additional dependency and interdependency analysis and resiliency effort with all 16 currently defined NIPP sectors. This, in turn, could create higher ordered tiers within the HSIB.

Tiered implementation of a geographic regional structure[101] within the HSIB—such as those previously noted or the six U.S. Department of Justice Regional Information Sharing System (RISS) geographic regions[102] or the 10 established FEMA (federal) geographic regions[103]—might further serve to better manage security and resilience issues and initiatives and may facilitate a clearer understanding of the intra- and inter-regional risk landscape and operating environments as contemplated by former DHS Secretary Michael Chertoff.[104] Federal resources and programs, such as the federal protective security advisors (currently aligned by the established federal regions), the cyber security advisors

---

[99] U.S. Department of Homeland Security, *National Protection Framework*, 22.

[100] Egli, *Beyond the Storms*, 30.

[101] Hardenbrook, "The Need for a Policy Framework," 7.

[102] U.S. Department of Justice, *Regional Information Sharing Systems (RISS) Program* [brochure] (Washington, DC: U.S. Department of Justice, 2014), accessed December 5, 2014, https://www.riss.net/default/Overview.

[103] "Regional Operations: FEMA Regional Offices," Federal Emergency Management Agency, accessed December 5, 2014, https://www.fema.gov/regional-operations.

[104] U.S. Department of Homeland Security, *National Infrastructure Protection Plan*, i–ii.

(CSA), the Regional Resiliency Assessment Program (RRAP),[105] and the National Infrastructure Simulation and Assessment Center (NISAC), could be systematically engaged[106] with SLTT practitioners and partners across the HSIB tiers and regions. Establishing a HSIB with such a regional construct is consistent with the NIPP 2013 core tenets 1–5 (specifically Core Tenet 5).[107] Such a construct may create a clearer regional identity for state and local infrastructure practitioners and partners. It may also provide the necessary multijurisdictional regional management structure and strategic mission space to facilitate and operationally achieve goals, such as the 12 innovative risk management and the partnership building *calls to action* included in the NIPP 2013[108]—all of the goals have a multijurisdictional or regional dimension—or the forward-looking implementation of the FEMA 2030 vision of *Essential Capabilities*, *Innovative Models & Tools* and *Dynamic Partnerships* of crisis and disaster response.[109] Additionally, this construct could support and integrate with existing regional consortia[110] and further institutionalize our largely voluntary protection mission space (see Table 5).[111] Existing fusion centers within each state could further reinforce this thinking as coordinating nodes within a regional HSIB construct and could be definitely linked to the National Infrastructure

[105] Federal Emergency Management Agency, *Fiscal Year 2014 Homeland Security Grant Program Supplemental Resource* (Washington, DC: Federal Emergency Management Agency, 2014), http://www.fema.gov/media-library-data/1395243947274-507831e9fb40d412030789b609a555bc/FY%202014%20Supplemental%20Guidance_Regional%20Resiliency%20Assessment%20Program_Final.pdf, 1–4.

[106] Egli, *Beyond the Storms*, 22, 73, 85.

[107] U.S. Department of Homeland Security, *NIPP 2013*, 13.

[108] Ibid., 21–26.

[109] Federal Emergency Management Agency, *Crisis Response and Disaster Resilience 2030: Forging Strategic Action in an Age of Uncertainty: Progress Report Highlighting the 2010–2011 Insights of the Strategic Foresight Initiative* (Washington, DC: Federal Emergency Management Agency, 2012), 13–20.

[110] U.S. Department of Homeland Security, *National Infrastructure Protection Plan*, i.

[111] Ibid.

Coordinating Center (NICC) and the National Cybersecurity and Communications Integration Center (NCCIC) for this purpose.[112]

Table 5. Summary of key findings aligned to recommendations: HSIB (C)

FINDING	A. Funding	B. Alignment	**C. HSIB**
There is a lack of dedicated and consistent CIP (security and resilience) program funding.	X		
There is a lack of dedicated and mature tactical CIP (security and resilience) organizations at or within the SLTT levels of government.	X	X	
There is a lack of dedicated and consistent CIP (security and resilience) program staffing.	X	X	
There is significant variation in the consistency and local adaptation with which the CIP (security and resilience) mission is interpreted, understood, applied and implemented across the nation.		X	**X**

[112] U.S. Department of Homeland Security, *NIPP Supplemental Tool*, 2, 7.

VII. CONCLUSION

Is there a problem here? There appears to be an interesting paradox in the respondent data. State and local jurisdictions and the professionals that serve them appear to be getting the job done from an operational perspective—operational tools, as needed operational staffing and tactical organizational models do exist. However, respondents report that the development of clear management constructs, tactical business processes, and associated tactical CIP (security and resilience) organizations to manage those processes and be wholly dedicated to support this mission space within state and local jurisdictions has been modest.

The respondent data appears to indicate a lack of available, dedicated, and consistently applied CIP (security and resilience) program funding and CIP (security and resilience) program staff. The respondent data also appears to illustrate that the CIP (security and resilience) mission is highly adapted locally and is not clearly and/or consistently interpreted, understood, applied, or implemented across the nation.

There are several opportunities to strengthen the systemic support structure and foster consistent maturing of tactical CIP (security and resilience) organizations nationally. Further availability of sustained and targeted federal funding to SLTT critical infrastructure security and resilience organizations may be the most viable national approach to ensure the most uniformed and even development and implementation of tactical organizations and programs across the nation because of the federal government's ability to craft new grant funding availabilities or to reshape the priorities and application of existing and currently available grant funds.

Additionally, based on survey responses, closer and formalized organizational and/or programmatic alignment within SLTT jurisdictions of the CIP/risk management mission to the mitigation and preparedness mission space

of emergency management should be explored. From a doctrinal and organizational perspective, the United States appears to generally maintain critical infrastructure protection (security and resilience) and emergency management as two discrete (in some cases almost mutually exclusive) parallel workflows. This organizational separation may be very necessary, appropriate, and sustainable within the context of federal and state governments. Based on respondent data, it appears that the need or sustainability of discrete and/or parallel critical infrastructure protection (security and resilience) and other public safety (i.e., law enforcement and emergency management) organizations softens with the more local levels of government. Respondent data indicates that local adaptation[113] of blended organizations and associated blended responsibilities appears to be currently prevalent. Although in many instances emergency management organizations can be understaffed and/or under-resourced—based on respondent data—it appears that both critical infrastructure protection (security and resilience) and emergency management partners across the state and local government spectrum would embrace such an alignment. The more mature root system of the emergency management preparedness and mitigation space could serve critical infrastructure protection (security and resilience) practitioners well.

The creation of a Homeland Security Industrial Base (HSIB), initially comprised of the defined lifeline infrastructure sectors, could bring a sharper programmatic focus to intra- and inter-regional critical infrastructure protection and resiliency (CIPR) activities generally and specifically within and among these infrastructure sectors and therefore should be explored and considered. The integration of a HSIB with DPA mandates and authorities could also serve to eliminate or bridge much of the artificial distinctions that currently exist between military and civilian doctrine. Integrated national doctrine should result in sharpened national programmatic focus on a more finite scope of “critical” infrastructure sectors, which will allow the multi-jurisdictional CIPR mission to be

[113] Sagarin, “Natural Security for a Variable and Risk-Filled World,” 6–8.

more clearly interpreted, understood, programmatically consumable and facilitate a steady-state protection and resilience posture.[114]

Tiered implementation of a geographic regional structure[115] within the HSIB might further serve to better manage security and resilience issues, initiatives, and programs and may facilitate a clearer multijurisdictional understanding of the intra- and inter-regional risk landscape and operating environments.[116] Federal resources and programs (civilian and military), could be systematically engaged[117] with SLTT practitioners and partners across the HSIB tiers and regions. Moreover, the Homeland Security Industrial Base could serve the needs of our national defense complex as well as the commercial and economic needs of state and local communities; therefore, it would serve to further strengthen the commercial and economic fabric of the nation and remain true to our federalist system.

As individual or coupled elements, enhanced funding opportunities, strengthened tactical CIP (security and resilience) organizations, and a refined strategic regional implementation approach could better support consistent programmatic implementation nationally. This could mitigate any conditions of national TOC that may potentially exist or emerge and further drive a national multidiscipline multijurisdictional culture of steady-state resilience.

---

[114] U.S. Department of Homeland Security, *National Protection Framework*, 22.

[115] Hardenbrook, “The Need for a Policy Framework,” 7.

[116] U.S. Department of Homeland Security, *National Infrastructure Protection Plan*, i–ii.

[117] Egli, *Beyond the Storms*, 22, 73, 85.

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX A. THE SURVEY QUESTIONS

Putting the Critical Back in Critical Infrastructure

The purpose of this survey and its associated research is to study critical infrastructure protection activities, in state and local government that illustrate the level of programmatic and organizational maturity and establishment.

You are invited to participate in this research study titled “Putting the Critical Back in Critical Infrastructure.” This survey will be conducted via Lime Survey. Only answers to survey questions will be collected. No personal identifying data will be collected or stored. Survey responses will be presented anonymously to the researcher. There is minimal risk that data collected could be mismanaged. THANK YOU for your interest and time!

There are 48 questions in this survey.

Question One
You are invited to participate in this research study titled “Putting the Critical Back in Critical Infrastructure.” The purpose of the research is to study critical infrastructure protection activities in state and local government that illustrate the level of programmatic and organizational maturity and establishment.

This survey will be conducted via Lime Survey. Only answers to survey questions will be collected. No personal identifying data will be collected or stored. Survey responses will be presented anonymously to the Researcher. There is minimal risk that data collected could be mismanaged.

This survey is expected to take 20–25 minutes to complete. Your participation is voluntary. If you participate, you are free to skip any question(s) or stop participating at any time without penalty or consequence. The alternative to participating is to not participate, which you may choose by clicking the “I do not consent to participate in this study” button below. Your responses to the survey are anonymous and no personally identifiable information will be collected or captured. All survey related material will be kept on a password-protected computer, which will be locked in an office or file cabinet. At the conclusion of this research, all survey related data will be turned over to the principal investigator and kept on a password-protected computer that will be locked in an office.

The anticipated benefit of this study is to add to the body of research about best practices to meet the emerging needs for state and local critical infrastructure protection practitioners and organizations and to gain insight into the current state of maturity of critical infrastructure protection practices and organizations. You may receive a copy of the completed research by contacting the researcher at bcmason@nps.edu. Contacting the researcher does not affect the anonymity of your participation in the study.

If you have questions about this research, contact the Naval Postgraduate School principal investigator Rudy Darken at darken@nps.edu. If you have questions regarding your rights as a research subject, contact the Naval Postgraduate School, Institutional Review Board (IRB) Chair Dr. Larry Shattuck at lgshattu@nps.edu or 831 656 2473.

Please choose **only one** of the following:

- I consent to participate in this study.
- I do not consent to participate in this study.

Question Two
I am:
Please choose **only one** of the following:

- a critical infrastructure protection (CIP) practitioner within my jurisdiction.
- a member of a partner organization to my jurisdiction's CIP practitioners.

Question Three
My primary jurisdiction is or within the state/territory of:
Please choose **only one** of the following:

- Alabama
- Alaska
- American Samoa
- Arizona
- Arkansas
- California
- Colorado
- Connecticut
- Delaware
- District of Columbia
- Federated States of Micronesia
- Florida
- Georgia
- Guam
- Hawaii
- Idaho
- Illinois
- Indiana
- Iowa
- Kansas
- Kentucky
- Louisiana
- Maine
- Maryland
- Massachusetts
- Michigan
- Minnesota
- Mississippi
- Missouri
- Montana
- Nebraska
- Nevada
- New Hampshire
- New Jersey
- New Mexico
- New York
- North Carolina
- North Dakota
- Northern Mariana Islands

- Ohio
- Oklahoma
- Oregon
- Pennsylvania
- Puerto Rico
- Republic of the Marshall Islands
- Rhode Island
- South Carolina
- South Dakota
- Tennessee
- Texas
- United States Virgin Islands
- Utah
- Vermont
- Virginia
- Washington
- West Virginia
- Wisconsin
- Wyoming

Question Four
My organization is best described by one of the following:
Please choose **only one** of the following:

- Critical infrastructure protection (CIP)
- Emergency management
- Emergency medical services (EMS)
- Fire / rescue / hazardous materials
- Homeland security
- Information technology (IT) / cybersecurity
- Law enforcement
- Private sector infrastructure owner / operator
- Public health
- Public works
- Utilities regulator
- Other—please describe in the narrative box provided

Make a comment on your choice here: NARRATIVE BOX PROVIDED

Question Five

Please choose one of the following that best describes your role within your organization:
Please choose **only one** of the following:

- Program manager
- Supervisor / team leader
- Manager / bureau chief
- Director / deputy director
- Elected public official
- Appointed public official
- Vice president / managing director / executive manager
- Other—please describe in the narrative box provided

Make a comment on your choice here: NARRATIVE BOX PROVIDED

Question Six
Please choose one of the following that best describes how long you have been a CIP practitioner or CIP partner:
Please choose **only one** of the following:

- 1–5 years
- 6–10 years
- 11–15 years
- 16–20 years
- more than 20 years

Question Seven
My jurisdiction is:

Please choose **only one** of the following:

- City / town / village / municipal
- County / parish
- State
- Territorial
- Tribal
- Private sector infrastructure owner / operator
- Other—please describe in the narrative box provided

Make a comment on your choice here: NARRATIVE BOX PROVIDED

Question Eight
Please choose one of the following that best describes your jurisdiction:

Please choose **only one** of the following:

- Rural
- Rural—suburban
- Suburban
- Suburban—urban
- Urban

Question Nine
The function of protecting critical infrastructure (CI) against all hazards in the United States has become a professional discipline.
Please choose the appropriate response for each item: PLEASE SELECT ONE

Strongly Disagree	Disagree	Somewhat Disagree	Somewhat Agree	Agree	Strongly Agree

Question Ten
The function of protecting critical infrastructure against all hazards in the United States SHOULD become (or be maintained as) a professional discipline.

Please choose the appropriate response for each item: PLEASE SELECT ONE

Strongly Disagree	Disagree	Somewhat Disagree	Somewhat Agree	Agree	Strongly Agree

Question Eleven
My elected chief executive (e.g., mayor, governor) and/or elected governing body (e.g., council, committee, commission, board, legislature) have issued EXECUTIVE ORDERS and/or enacted LEGISLATION regarding CIP and/or related program authorities / requirements.

Please choose the appropriate response for each item: PLEASE SELECT ONE

Strongly Disagree	Disagree	Somewhat Disagree	Somewhat Agree	Agree	Strongly Agree

Question Twelve
The CIP organization in my jurisdiction utilizes the concepts outlined in the *National* Infrastructure *Protection Plan* (NIPP).

Please choose the appropriate response for each item: PLEASE SELECT ONE

Strongly Disagree	Disagree	Somewhat Disagree	Somewhat Agree	Agree	Strongly Agree

Question Thirteen
My jurisdiction maintains a CIP all hazards strategic plan.
Please choose the appropriate response for each item: PLEASE SELECT ONE

No	Yes	I Don't Know

No	Yes	I Don't Know

Question Fourteen
The CIP organization in my jurisdiction maintains a productive working relationship with the U.S. Department of Homeland Security (DHS) protective security advisor (PSA) assigned to my jurisdiction.

Please choose the appropriate response for each item: PLEASE SELECT ONE

Strongly Disagree	Disagree	Somewhat Disagree	Somewhat Agree	Agree	Strongly Agree	I DON'T KNOW

Question Fifteen
My jurisdiction uses a method for measuring (e.g., performance measures or returns on investment) the effectiveness of the CIP program.

Please choose the appropriate response for each item: PLEASE SELECT ONE

Strongly Disagree	Disagree	Somewhat Disagree	Somewhat Agree	Agree	Strongly Agree	I DON'T KNOW

Question Sixteen
There are many infrastructure assets, facilities and/or systems in my jurisdiction that require protection against all hazards.

Please choose the appropriate response for each item: PLEASE SELECT ONE

Strongly Disagree	Disagree	Somewhat Disagree	Somewhat Agree	Agree	Strongly Agree

Question Seventeen
The CIP program in my jurisdiction is responsible for developing and/or implementing risk mitigation strategies for PUBLICLY owned or operated CI in my jurisdiction.

Please choose the appropriate response for each item: PLEASE SELECT ONE

	No	Yes	I Don't Know

Question Eighteen
Please estimate the percentage of critical infrastructure that are PUBLICLY owned or operated in your jurisdiction.

Please choose **only one** of the following:

- 0%
- 5%
- 10%
- 15%
- 20%
- 25%
- 30%
- 35%
- 40%
- 45%
- 50%
- 55%
- 60%
- 65%
- 70%
- 75%
- 80%
- 85%
- 90%
- 95%
- 100%

Question Nineteen
My jurisdiction maintains a CIP organizational element (e.g., team, unit, group, bureau, division, department) fully dedicated to the mission of protecting critical infrastructure in my jurisdiction.

Please choose the appropriate response for each item: PLEASE SELECT ONE

	No	Yes	I Don't Know

Question Twenty
The CIP / risk management mission should be more closely aligned to the mitigation and preparedness mission space of emergency management.

Please choose the appropriate response for each item: PLEASE SELECT ONE

Strongly Disagree	Disagree	Somewhat Disagree	Somewhat Agree	Agree	Strongly Agree

Question Twenty-One
My organization / jurisdiction maintains FULLTIME staff dedicated to the CIP mission.
Please choose **only one** of the following:

- No
- Yes
- I Don't Know

Question Twenty-Two
Approximately how many FULLTIME staff members are dedicated to the CIP mission in your organization / jurisdiction?

Please choose **only one** of the following:

- 1
- 2
- 3
- 4
- 5
- 6
- 7
- 8
- 9
- 10
- 11
- 12
- 13
- 14
- 15
- 16
- 17
- 18
- 19
- 20
- 21
- 22
- 23
- 24
- 25 +

Question Twenty-Three
My organization / jurisdiction maintains PART-TIME staff dedicated to the CIP mission.

Please choose **only one** of the following:

- No
- Yes
- I don't know

Question Twenty-Four
Approximately how many PART-TIME staff members are dedicated to the CIP mission in your organization / jurisdiction?

Please choose **only one** of the following:

- 1
- 2
- 3
- 4
- 5
- 6
- 7
- 8
- 9
- 10
- 11
- 12
- 13
- 14
- 15
- 16
- 17
- 18
- 19
- 20
- 21
- 22
- 23
- 24
- 25 +

Question Twenty-Five
The CIP program / organization in my jurisdiction is adequately staffed.

Please choose the appropriate response for each item: PLEASE SELECT ONE

	Strongly Disagree	**Disagree**	**Somewhat Disagree**	**Somewhat Agree**	**Agree**	**Strongly Agree**	**I DON'T KNOW**

Question Twenty-Six
The staff members assigned to CIP responsibilities in my jurisdiction are appropriately trained.

Please choose the appropriate response for each item: PLEASE SELECT ONE

	Strongly Disagree	**Disagree**	**Somewhat Disagree**	**Somewhat Agree**	**Agree**	**Strongly Agree**	**I DON'T KNOW**

Question Twenty-Seven

The salaries of staff members assigned to CIP responsibilities in my jurisdiction are funded by: (please enter only whole numbers—if you do not know, please enter "0" next to "I don't know")

Please enter your answer(s) here:

- My jurisdiction’s operational budget (%)
- The private sector (%)
- State financial grants (%)
- Federal financial grants (%)
- Other (%)
- I don't know—please enter "0"

Question Twenty-Eight
Regarding staff members salaries assigned to CIP responsibilities in your jurisdiction that are supported by FEDERAL grant funding, please select all that apply and indicate the percentage of financial dependence:(please enter whole numbers —if you do not know, please enter a "0" next to "I don't know")
Please enter your answer(s) here:

- Emergency Management Performance Grant (EMPG) (%)
- Homeland Security Grant Program (HSGP) (%)
- Urban Areas Security Initiative (UASI) (%)
- Port Security Grant Program (PSGP) (%)
- Transit Security Grant Program (TSGP))%)
- Centers for Disease Control and Preparedness (CDC) (%)
- Other (%)
- I don't know—please enter "0"

Question Twenty-Nine
The CIP program in my jurisdiction is managed by an organizational component that is ENTIRELY dedicated to critical infrastructure protection as its core mission.

Please choose the appropriate response for each item: PLEASE SELECT ONE

	Strongly Disagree	**Disagree**	**Somewhat Disagree**	**Somewhat Agree**	**Agree**	**Strongly Agree**	**I DON'T KNOW**

Question Thirty

The CIP program in my jurisdiction is managed as a COLLATERAL responsibility by an organizational component whose core mission is NOT critical infrastructure protection.

Please choose the appropriate response for each item: PLEASE SELECT ONE

Strongly Disagree	Disagree	Somewhat Disagree	Somewhat Agree	Agree	Strongly Agree	I DON'T KNOW

Question Thirty-One
The CIP program in my jurisdiction maintains designated liaisons / relationship managers / coordinators to work with critical infrastructure owners and/or operators.

Please choose the appropriate response for each item: PLEASE SELECT ONE

Strongly Disagree	Disagree	Somewhat Disagree	Somewhat Agree	Agree	Strongly Agree	I DON'T KNOW

Question Thirty-Two
The CIP program in my jurisdiction utilizes its own criteria to identify assets of significance to my jurisdiction.

Please choose the appropriate response for each item: PLEASE SELECT ONE

No	Yes	I Don't Know

Question Thirty-Three
The CIP program in my jurisdiction employs a method to identify critical infrastructure assets, systems, and/or networks that may be at risk.

Please choose the appropriate response for each item: PLEASE SELECT ONE

Strongly Disagree	Disagree	Somewhat Disagree	Somewhat Agree	Agree	Strongly Agree

Question Thirty-Four

The CIP program in my jurisdiction conducts sector and/or site specific risk assessments that include threat, vulnerability, and consequence.

Please choose the appropriate response for each item: PLEASE SELECT ONE

Strongly Disagree	Disagree	Somewhat Disagree	Somewhat Agree	Agree	Strongly Agree

Question Thirty-Five
The CIP program in my jurisdiction maintains sector relationships through established sector working groups or coordinating councils.

Please choose the appropriate response for each item: PLEASE SELECT ONE

Strongly Disagree	Disagree	Somewhat Disagree	Somewhat Agree	Agree	Strongly Agree

Question Thirty-Six
The CIP program in my jurisdiction maintains an engagement model with infrastructure owners and operators DIFFERENT from sector working groups or coordinating councils. IF YES, please describe in the narrative box provided.

Please choose **only one** of the following:

- No
- Yes (please describe in narrative box provided)
- I don't know

Make a comment on your choice here: NARRATIVE BOX PROVIDED

Question Thirty-Seven
Please select one of the following that best describes how often the CIP program in your jurisdiction meets with infrastructure owners and operators.

Please choose the appropriate response for each item: PLEASE SELECT ONE

Never	Almost Never	Infrequently	Occasionally	Frequently	Very Frequently	I DON'T KNOW

Question Thirty-Eight
The CIP MISSION in my jurisdiction is well understood by stakeholders (e.g., private and public sector infrastructure owners/operators, other governmental partners).

Please choose the appropriate response for each item: PLEASE SELECT ONE

Strongly Disagree	Disagree	Somewhat Disagree	Somewhat Agree	Agree	Strongly Agree

Question Thirty-Nine
The CIP ORGANIZATION in my jurisdiction is well understood by stakeholders (private and public sector infrastructure owners/operators as well as other governmental partners).

Please choose the appropriate response for each item: PLEASE SELECT ONE

Strongly Disagree	Disagree	Somewhat Disagree	Somewhat Agree	Agree	Strongly Agree

Question Forty
The CIP program in my jurisdiction maintains mature and well-defined programmatic GOALS, OBJECTIVES, and related BUSINESS PROCESSES.

Please choose the appropriate response for each item: PLEASE SELECT ONE

Strongly Disagree	Disagree	Somewhat Disagree	Somewhat Agree	Agree	Strongly Agree	I DON'T KNOW

Question Forty-One
The CIP program in my jurisdiction shares information with infrastructure owners and operators.

Please choose the appropriate response for each item: PLEASE SELECT ONE

Strongly Disagree	Disagree	Somewhat Disagree	Somewhat Agree	Agree	Strongly Agree	I DON'T KNOW

Question Forty-Two
Infrastructure owners and operators in my jurisdiction share information with the CIP program.

Please choose the appropriate response for each item: PLEASE SELECT ONE

Strongly Disagree	Disagree	Somewhat Disagree	Somewhat Agree	Agree	Strongly Agree	I DON'T KNOW

Question Forty-Three
The CIP mission has been FULLY IMPLEMENTED in my jurisdiction.

Please choose the appropriate response for each item: PLEASE SELECT ONE

Strongly Disagree	Disagree	Somewhat Disagree	Somewhat Agree	Agree	Strongly Agree

Question Forty-Four
The CIP mission has been IMPLEMENTED WELL in my jurisdiction.

Please choose the appropriate response for each item: PLEASE SELECT ONE

Strongly Disagree	Disagree	Somewhat Disagree	Somewhat Agree	Agree	Strongly Agree

Question Forty-Five
The CIP mission is WELL MANAGED in my jurisdiction.

Please choose the appropriate response for each item: PLEASE SELECT ONE

Strongly Disagree	Disagree	Somewhat Disagree	Somewhat Agree	Agree	Strongly Agree

Question Forty-Six
Given the risk, every reasonable measure has been taken to assure the critical infrastructure in my jurisdiction is WELL PROTECTED.

Please choose the appropriate response for each item: PLEASE SELECT ONE

Strongly Disagree	Disagree	Somewhat Disagree	Somewhat Agree	Agree	Strongly Agree

Question Forty-Seven
My jurisdiction has shifted the focus from critical infrastructure “PROTECTION” to also include critical infrastructure “RESILIENCY.”

Please choose the appropriate response for each item: PLEASE SELECT ONE

Strongly Disagree	Disagree	Somewhat Disagree	Somewhat Agree	Agree	Strongly Agree

Question Forty-Eight
If there was one thing that could be done in your jurisdiction to improve the CIP program, what would that be?

Please write your answer here: NARRATIVE BOX PROVIDED

THANK YOU !

WWW.CHDS.US

Submit your survey.
Thank you for completing this survey.

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX B. RAW DATA TABLES

QUESTION 1

Response	Number of Respondents
No response provided	*0*
I consent	91
I do not consent	0

QUESTION 2

Response	Number of Respondents
No response provided	*1*
CIP practitioner	61
Partner	29

QUESTION 3

Response	Number of Respondents
No response provided	*1*
Alabama	1
Alaska	0
American Samoa	0
Arizona	2
Arkansas	1
California	11
Colorado	3
Connecticut	1
Delaware	0
District of Columbia	3
Federated States of Micronesia	0
Florida	12
Georgia	0
Guam	0
Hawaii	0
Idaho	1
Illinois	1
Indiana	1

Iowa	0
Kansas	0
Kentucky	2
Louisiana	2
Maine	1
Maryland	0
Massachusetts	0
Michigan	5
Minnesota	2
Mississippi	0
Missouri	1
Montana	0
Nebraska	1
Nevada	3
New Hampshire	1
New Jersey	3
New Mexico	1
New York	4
North Carolina	0
North Dakota	0
Northern Mariana Islands	0
Ohio	2
Oklahoma	4
Oregon	1
Pennsylvania	4
Puerto Rico	0
Republic of the Marshall Islands	0
Rhode Island	0
South Carolina	0
South Dakota	1
Tennessee	0
Texas	4
United States Virgin Islands	0
Utah	0
Vermont	0
Virginia	2
Washington	8
West Virginia	0
Wisconsin	1
Wyoming	0

QUESTION 4

Response	Number of Respondents
No response provided	*0*
Critical infrastructure protection (CIP)	8
Emergency management	32
Emergency medical services	1
Fire / rescue / hazardous materials	3
Homeland security	15
Information technology	0
Law enforcement	16
Private sector infrastructure owner / operator	1
Public health	3
Public works	1
Utilities regulator	0
Other—narrative box	11

QUESTION 5

Response	Number of Respondents
No response provided	*0*
Program manager	29
Supervisor / team leader	9
Manager / bureau chief	13
Director / deputy director	15
Elected public official	0
Appointed public official	3
Vice-president / managing director / executive manager	2
Other—narrative box	20

QUESTION 6

Response	Number of Respondents
No response provided	*1*
1–5 years	32
6–10 years	31
11–15 years	16
16–20 years	0
more than 20 years	11

QUESTION 7

Response	Number of Respondents
No response provided	*0*
City / town / village / municipal	22
County / parish	27
State	30
Territorial	0
Tribal	0
Private sector infrastructure owner / operator	0
Other—narrative box	12

QUESTION 8

Response	Number of Respondents
No response provided	*4*
Rural	2
Rural—suburban	23
Suburban	4
Suburban—urban	34
Urban	24

QUESTION 9

Assigned Value	Response	Number of Respondents
	No response provided	*1*
1	Strongly disagree	3
2	Disagree	9
3	Somewhat disagree	10
4	Somewhat agree	29
5	Agree	25
6	Strongly agree	14

QUESTION 10

Assigned Value	Response	Number of Respondents
	No response provided	*0*
1	Strongly disagree	2
2	Disagree	2

3	Somewhat disagree	6
4	Somewhat agree	17
5	Agree	29
6	Strongly agree	35

QUESTION 11

Assigned Value	Response	Number of Respondents
	No response provided	*0*
1	Strongly disagree	9
2	Disagree	18
3	Somewhat disagree	11
4	Somewhat agree	23
5	Agree	21
6	Strongly agree	9

QUESTION 12

Assigned Value	Response	Number of Respondents
	No response provided	*1*
1	Strongly disagree	1
2	Disagree	0
3	Somewhat disagree	2
4	Somewhat agree	20
5	Agree	46
6	Strongly agree	21

QUESTION 13

	Response	Number of Respondents
	No response provided	*0*
	I don't know	6
	No	26
	Yes	59

QUESTION 14

Assigned Value	Response	Number of Respondents
	No response provided	*0*
99	I don't know	4
1	Strongly disagree	1
2	Disagree	3
3	Somewhat disagree	4
4	Somewhat agree	10
5	Agree	24
6	Strongly agree	45

QUESTION 15

Assigned Value	Response	Number of Respondents
	No response provided	*0*
99	I don't know	5
1	Strongly disagree	2
2	Disagree	19
3	Somewhat disagree	14
4	Somewhat agree	24
5	Agree	20
6	Strongly agree	7

QUESTION 16

Assigned Value	Response	Number of Respondents
	No response provided	*0*
1	Strongly disagree	0
2	Disagree	1
3	Somewhat disagree	2
4	Somewhat agree	7
5	Agree	25
6	Strongly agree	56

QUESTION 17

Response	Number of Respondents
No response provided	*2*
I don't know	8
No	28
Yes	53

QUESTION 18

Response	Number of Respondents
No response provided	*6*
0%	1
5%	0
10%	4
15%	11
20%	11
25%	11
30%	5
35%	2
40%	3
45%	3
50%	6
55%	0
60%	2
65%	3
70%	3
75%	4
80%	7
85%	2
90%	3
95%	3
100%	1

QUESTION 19

Response	Number of Respondents
No response provided	*3*
I don't know	3
No	45
Yes	40

QUESTION 20

Assigned Value	Response	Number of Respondents
	No response provided	*5*
1	Strongly disagree	1
2	Disagree	5
3	Somewhat disagree	3
4	Somewhat agree	21
5	Agree	37
6	Strongly agree	19

QUESTION 21

Response	Number of Respondents
No response provided	*6*
I don't know	3
No	35
Yes	47

QUESTION 22

Survey logic rule applied—the appearance of Question 22 in the survey was predicated on a “Yes” answer in Question 21.

Response	Number of Respondents
1	21
2	7
3	2
4	2
5	3
6	3
7	1
8	0
9	0
10	2
11	0
12	0
13	0
14	2

15	0
16	0
17	0
18	0
19	0
20	2
21	0
22	0
23	0
24	0
25+	2

QUESTION 23

Response	Number of Respondents
No response provided	*6*
I don't know	7
No	54
Yes	24

QUESTION 24

Survey logic rule applied—the appearance of Question 24 in the survey was predicated on a “Yes” answer in Question 23.

Response	Number of Respondents
1	6
2	4
3	6
4	1
5	4
6	0
7	0
8	0
9	0
10	2
11	0
12	0
13	0
14	0
15	0
16	0

	17	0
	18	0
	19	0
	20	0
	21	0
	22	0
	23	0
	24	0
	25+	1

QUESTION 25

Assigned Value	Response	Number of Respondents
	No response provided	*5*
99	I don't know	2
1	Strongly disagree	21
2	Disagree	21
3	Somewhat disagree	20
4	Somewhat agree	9
5	Agree	12
6	Strongly agree	1

QUESTION 26

Assigned Value	Response	Number of Respondents
	No response provided	*6*
1	Strongly disagree	5
2	Disagree	10
3	Somewhat disagree	8
4	Somewhat agree	24
5	Agree	29
6	Strongly agree	9

QUESTION 27

Response	Number of Respondents					
PERCENTAGE	Operational Budget	Private Sector	State Financial Grants	Federal Financial Grants	OTHER	I Don't Know
0	25	49	49	13	50	51
5	0	0	0	2	0	0
10	1	0	0	1	0	0
15	1	0	0	1	1	0
20	1	0	1	2	0	0
25	0	0	0	0	0	0
30	2	0	0	0	0	0
35	0	0	0	0	0	0
40	0	1	0	2	0	0
45	0	0	0	0	0	0
50	3	0	0	4	0	0
55	0	0	0	0	0	0
60	2	0	0	0	0	0
65	0	0	0	0	0	0
70	0	0	0	3	0	0
75	0	0	0	0	0	0
80	2	0	1	1	0	0
85	1	0	0	0	0	0
90	0	1	0	0	0	0
95	1	0	0	0	0	0
100	12	0	0	22	0	0
TOTAL	51	51	51	51	51	51

Footnotes:
i. One respondent did not fully indicate all sources of funding (i.e., the percent of funding budget did not equal 100 percent). In this instance, the analysis assumed all unallocated budget to the "other" funding source.

QUESTION 28

Response	Number of Respondents							
PERCENTAGE	EMPG	HSGP	UASI	PSGP	TSGP	CDC	OTHER	I Don't Know
0	26	17	21	34	36	37	37	38
1	0	0	0	1	1	1	0	0
3	0	0	1	0	0	0	0	0
5	0	0	0	0	0	0	0	0
10	0	0	0	2	0	0	0	0
15	1	1	1	0	1	0	0	0
20	0	1	0	0	0	0	0	0
25	2	1	1	0	0	0	0	0
30	0	2	0	0	0	0	0	0
34	0	1	0	0	0	0	0	0
35	0	0	0	0	0	0	0	0
40	0	0	0	0	0	0	0	0
45	0	0	1	0	0	0	0	0
50	3	5	4	0	0	0	1	0
55	0	0	0	0	0	0	0	0
60	0	0	0	0	0	0	0	0
65	0	0	0	0	0	0	0	0
66	1	0	0	0	0	0	0	0
70	0	0	2	0	0	0	0	0
74	1	0	0	0	0	0	0	0
75	0	1	0	1	0	0	0	0
80	0	0	0	0	0	0	0	0
85	0	0	0	0	0	0	0	0
90	0	0	0	0	0	0	0	0
95	0	0	0	0	0	0	0	0
100	4	9	7	0	0	0	0	0
TOTAL	38	38	38	38	38	38	38	38

Footnotes:

i. Two respondents indicated sources of "federal financial grants" funding that did not equal 100 percent. The percentage reported under the Question 28 single Federal financial source (i.e., EMPG, HSGP, UASI) was the same percentage indicated for "federal financial grants" in Question 27. In this instance the analysis assumed 100 percent under the federal financial source reported rather than the percentage provided.

ii. Four respondents did not fully indicate the source of federal financial grant funding. The percentage of Federal financial sources (i.e., EMPG, HSPG, UASI) in Question 28 did not equal 100 percent. In this instance, the analysis assumed all unallocated budget to equal 100% was allocated to the "other" funding source.

iii. One respondent reported that 100 percent of federal financial grants were EMPG funds and an additional 100 percent of federal financial grants came from HSGP funds. In this instance, the analysis assumed that only 50 percent came from each source of federal funds.

QUESTION 29

Assigned Value	Response	Number of Respondents
	No response provided	*6*
99	I don't know	1
1	Strongly disagree	17
2	Disagree	28
3	Somewhat disagree	8
4	Somewhat agree	12
5	Agree	8
6	Strongly agree	11

QUESTION 30

Assigned Value	Response	Number of Respondents
	No response provided	*7*
99	I don't know	1
1	Strongly disagree	7
2	Disagree	17
3	Somewhat disagree	6
4	Somewhat agree	10
5	Agree	27
6	Strongly agree	16

QUESTION 31

Assigned Value	Response	Number of Respondents
	No response provided	*7*
99	I don't know	2
1	Strongly Disagree	6
2	Disagree	6
3	Somewhat disagree	6
4	Somewhat agree	18
5	Agree	27
6	Strongly agree	19

QUESTION 32

	Response	Number of Respondents
	No response provided	*7*
	I don't know	11
	No	28
	Yes	45

QUESTION 33

Assigned Value	Response	Number of Respondents
	No response provided	*8*
1	Strongly disagree	1
2	Disagree	4
3	Somewhat disagree	4
4	Somewhat agree	37
5	Agree	27
6	Strongly agree	10

QUESTION 34

Assigned Value	Response	Number of Respondents
	No response provided	*8*
1	Strongly disagree	2
2	Disagree	8
3	Somewhat disagree	6
4	Somewhat agree	19
5	Agree	31
6	Strongly agree	17

QUESTION 35

Assigned Value	Response	Number of Respondents
	No response provided	*9*
1	Strongly disagree	3
2	Disagree	7
3	Somewhat disagree	8
4	Somewhat agree	23
5	Agree	28
6	Strongly agree	13

QUESTION 36

	Response	Number of Respondents
	No response provided	*11*
	I don't know	15
	No	47
	Yes	18

QUESTION 37

Assigned Value	Response	Number of Respondents
	No response provided	*10*
99	I don't know	2
1	Never	1
2	Almost never	5
3	Infrequently	9
4	Occasionally	33
5	Frequently	21
6	Very frequently	10

QUESTION 38

Assigned Value	Response	Number of Respondents
	No response provided	*8*
1	Strongly disagree	4
2	Disagree	8
3	Somewhat disagree	23
4	Somewhat agree	32
5	Agree	13
6	Strongly agree	3

QUESTION 39

Assigned Value	Response	Number of Respondents
	No response provided	*9*
1	Strongly disagree	4
2	Disagree	7
3	Somewhat disagree	25
4	Somewhat agree	31
5	Agree	13
6	Strongly agree	2

QUESTION 40

Assigned Value	Response	Number of Respondents
	No response provided	*9*
99	I don't know	3
1	Strongly disagree	5
2	Disagree	9
3	Somewhat disagree	20
4	Somewhat agree	24
5	Agree	12
6	Strongly agree	9

QUESTION 41

Assigned Value	Response	Number of Respondents
	No response provided	*9*
99	I don't know	2
1	Strongly disagree	5
2	Disagree	3
3	Somewhat disagree	6
4	Somewhat agree	20
5	Agree	27
6	Strongly agree	19

QUESTION 42

Assigned Value	Response	Number of Respondents
	No response provided	*9*
99	I don't know	2
1	Strongly disagree	4
2	Disagree	5
3	Somewhat disagree	10
4	Somewhat agree	23
5	Agree	29
6	Strongly agree	9

QUESTION 43

Assigned Value	Response	Number of Respondents
	No response provided	*8*
1	Strongly disagree	9
2	Disagree	21
3	Somewhat disagree	20
4	Somewhat agree	20
5	Agree	10
6	Strongly agree	3

QUESTION 44

Assigned Value	Response	Number of Respondents
	No response provided	*8*
1	Strongly disagree	4
2	Disagree	18
3	Somewhat disagree	13
4	Somewhat agree	32
5	Agree	8
6	Strongly agree	8

QUESTION 45

Assigned Value	Response	Number of Respondents
	No response provided	*8*
1	Strongly disagree	6
2	Disagree	12
3	Somewhat disagree	13
4	Somewhat agree	33
5	Agree	13
6	Strongly agree	6

QUESTION 46

Assigned Value	Response	Number of Respondents
	No response provided	*8*
1	Strongly disagree	5
2	Disagree	16
3	Somewhat disagree	18
4	Somewhat agree	27
5	Agree	13
6	Strongly agree	4

QUESTION 47

Assigned Value	Response	Number of Respondents
	No response provided	*10*
1	Strongly disagree	4
2	Disagree	9
3	Somewhat disagree	7
4	Somewhat agree	35
5	Agree	15
6	Strongly agree	11

QUESTION 48

NARRATIVE ONLY ANSWER—PLEASE SEE TABLE 1

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX C. CROSS-ANALYZED SUPPORT GRAPHS

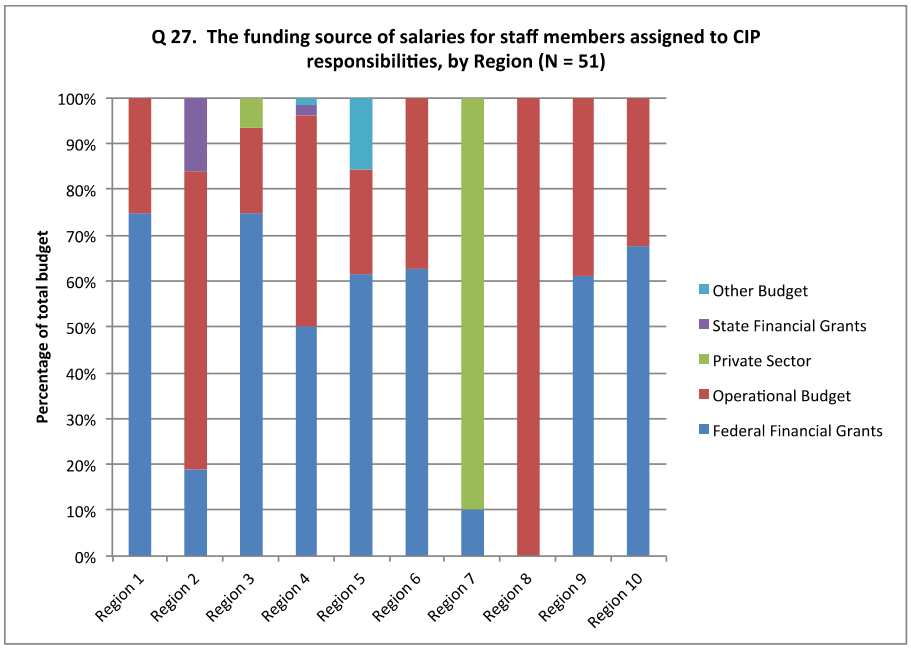


Figure 11A. CIP staff salary source by federal FEMA region.

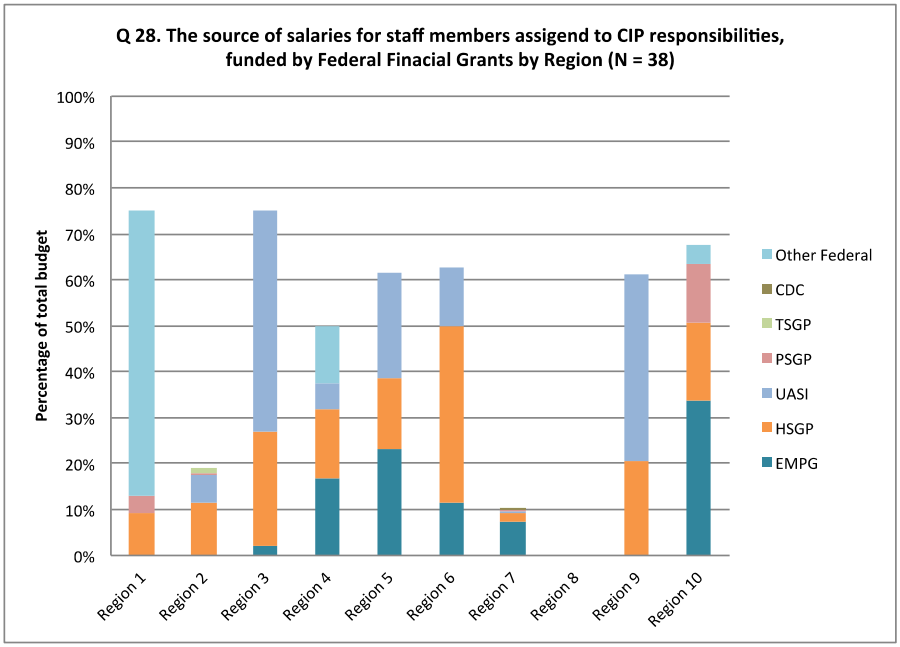


Figure 11B. Utilization of federal funds to support CIP staff salary by federal FEMA region.

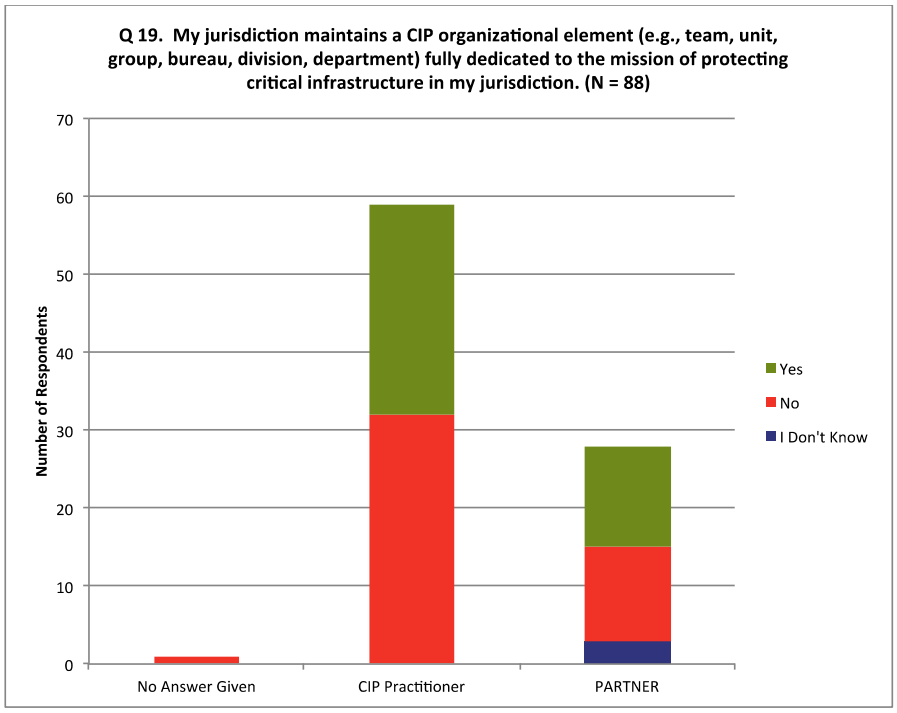


Figure 13A. Respondents' jurisdiction maintains a CIP organizational element fully dedicated to the CIP protection mission by practitioner and partner.

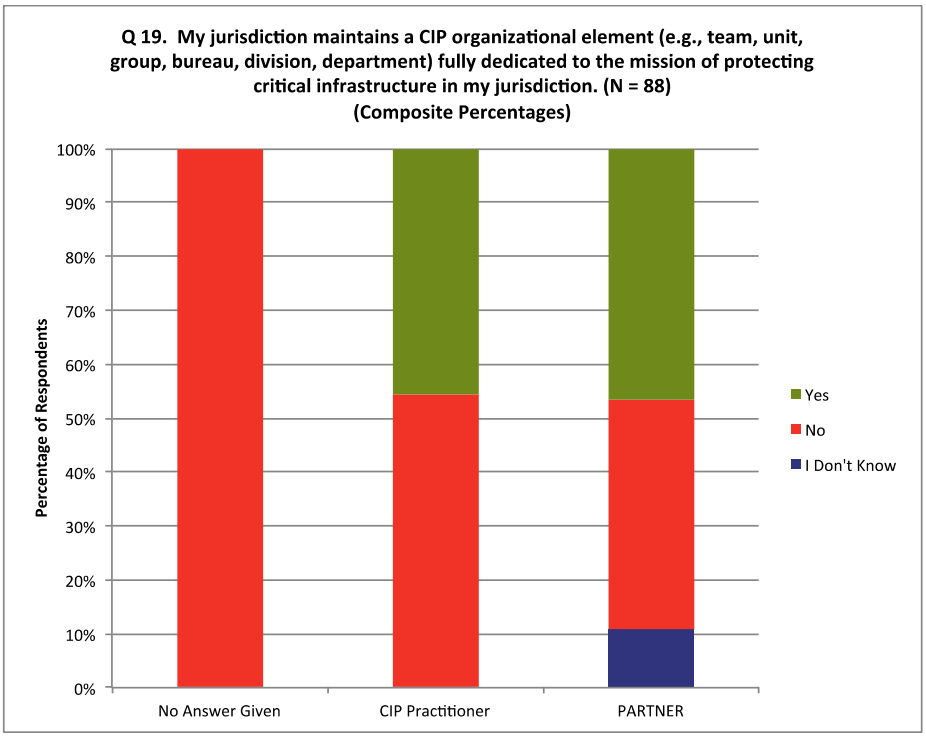


Figure 13B. Composite percentages of Figure 13A.

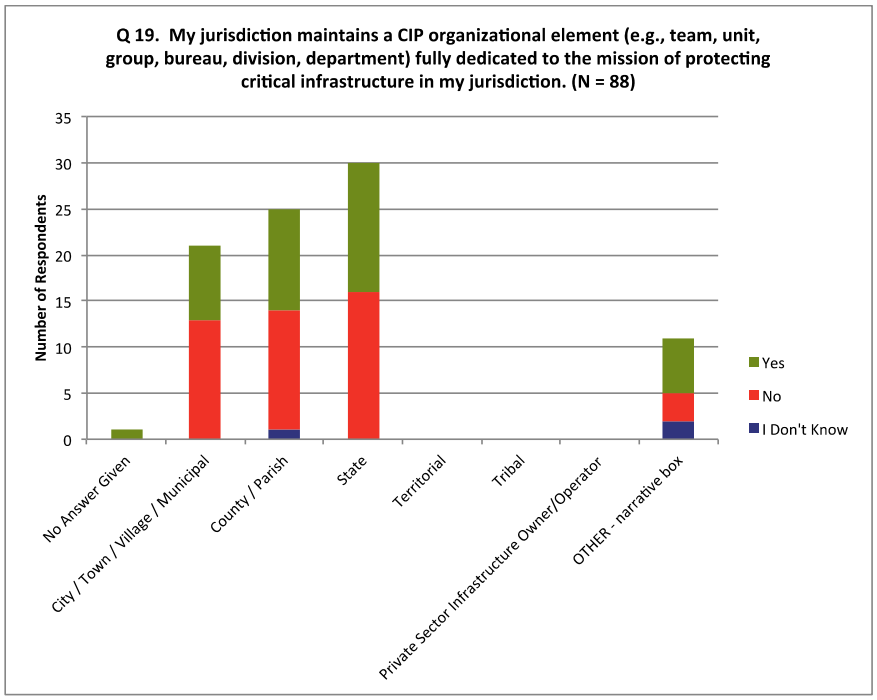


Figure 13C. Respondents' jurisdiction maintains a CIP organizational element fully dedicated to CIP protection mission by jurisdiction.

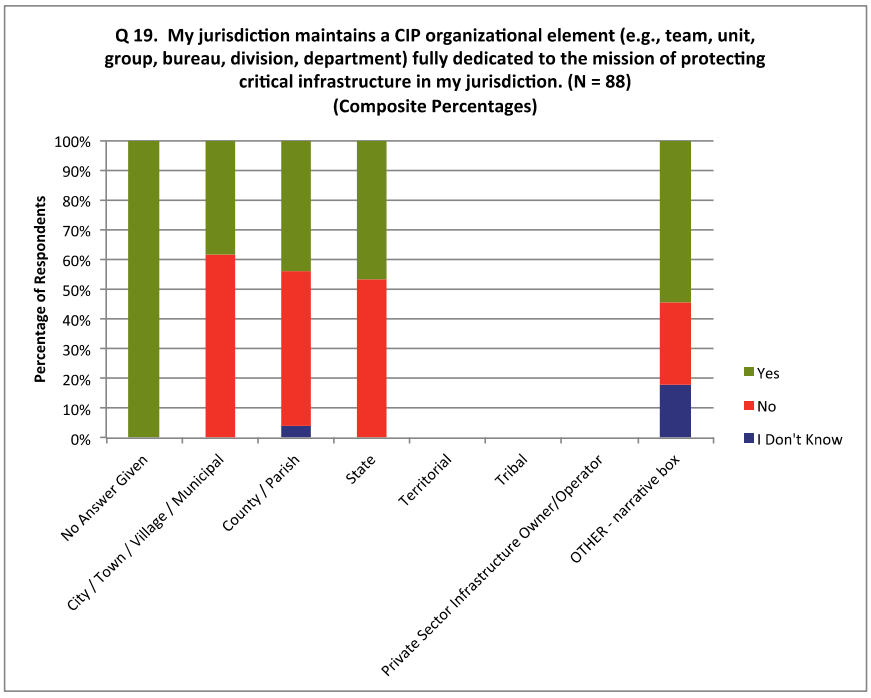


Figure 13D. Composite percentages of Figure 13C.

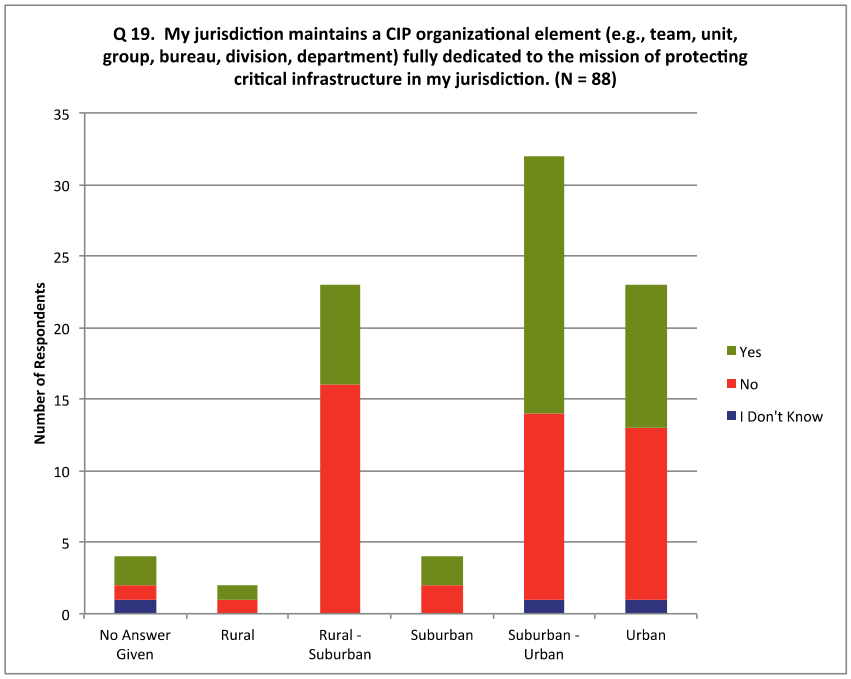


Figure 13E. Respondents' jurisdiction maintains a CIP organizational element fully dedicated to CIP protection mission by qualified jurisdiction.

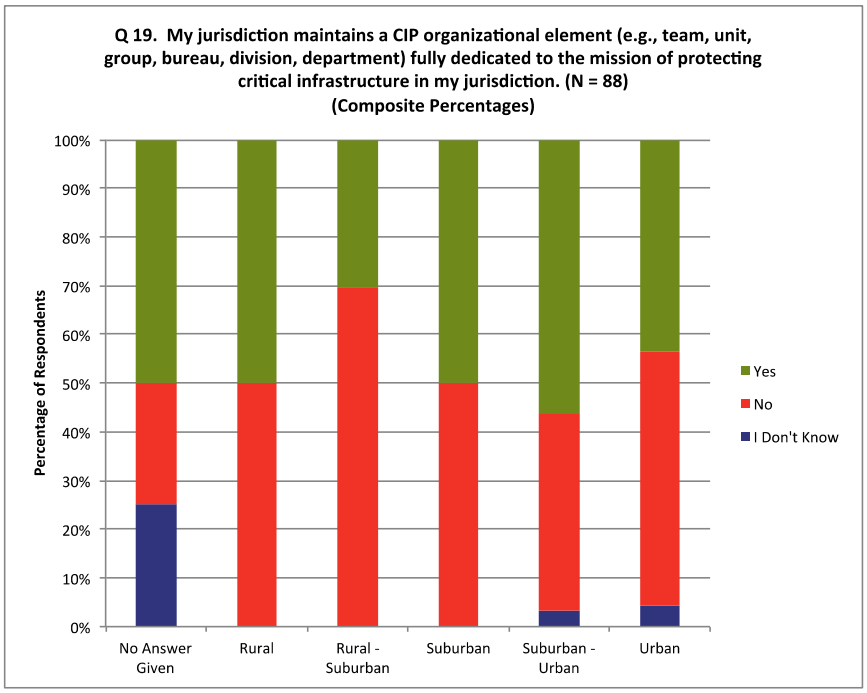


Figure 13F. Composite percentages of Figure 13E.

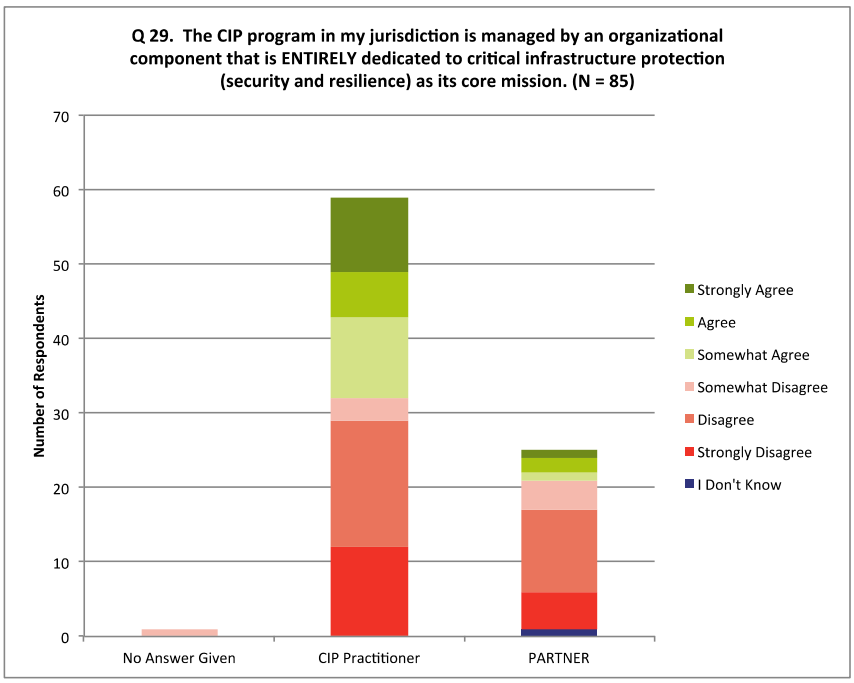


Figure 20A. Figure 20 cross-analyzed by respondents that self-identify as a CIP practitioner or partner.

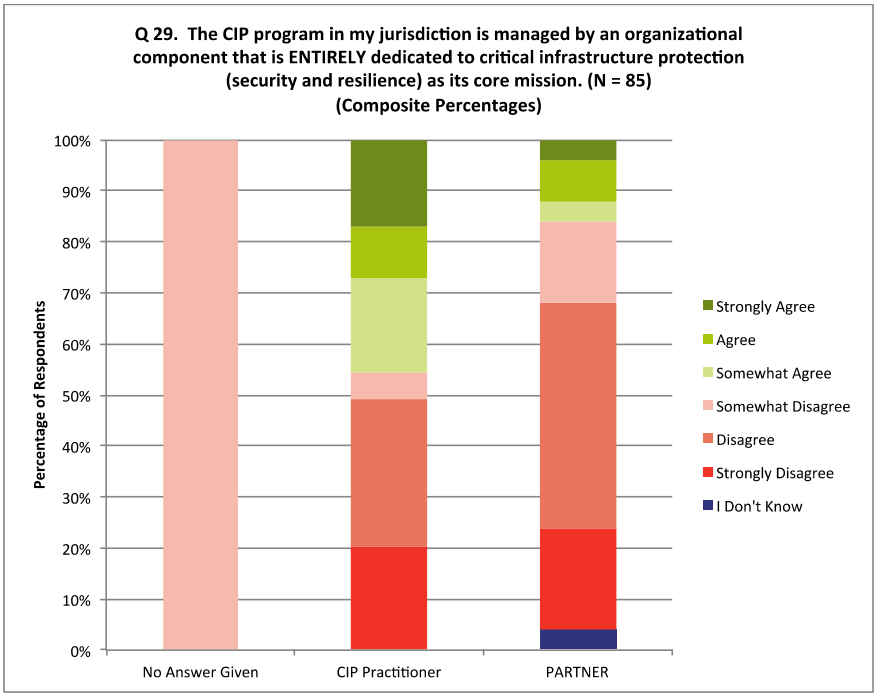


Figure 20B. Composite percentages of Figure 20A.

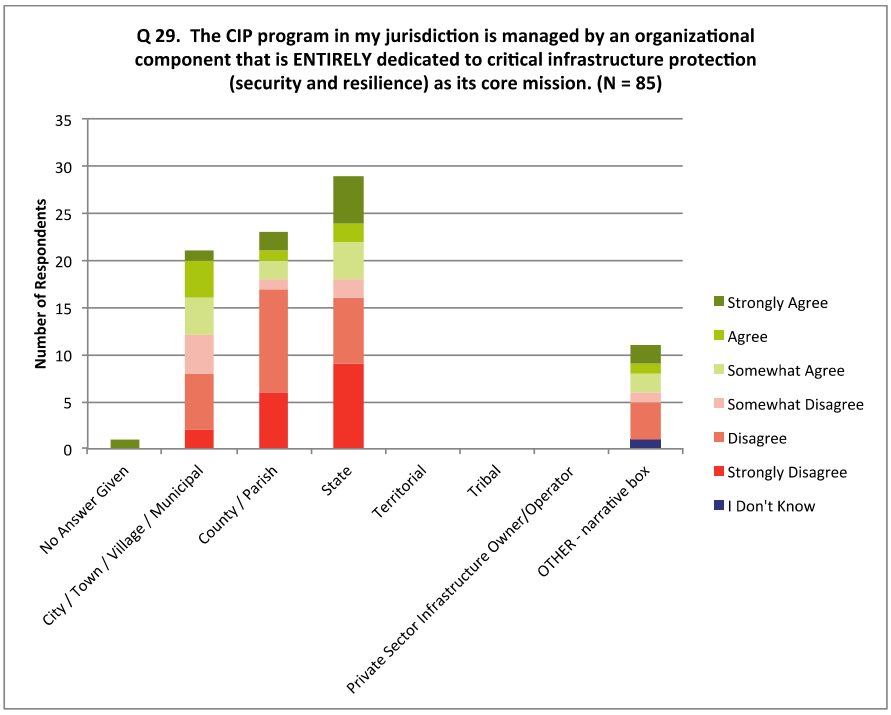


Figure 20C. Figure 20 cross-analyzed by respondents jurisdiction type.

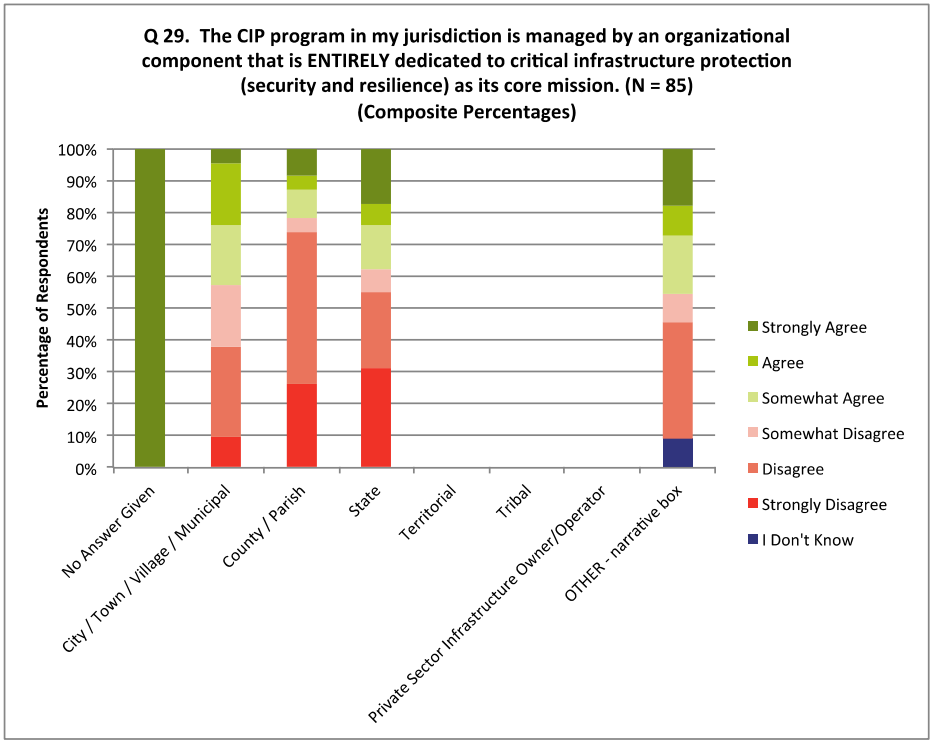
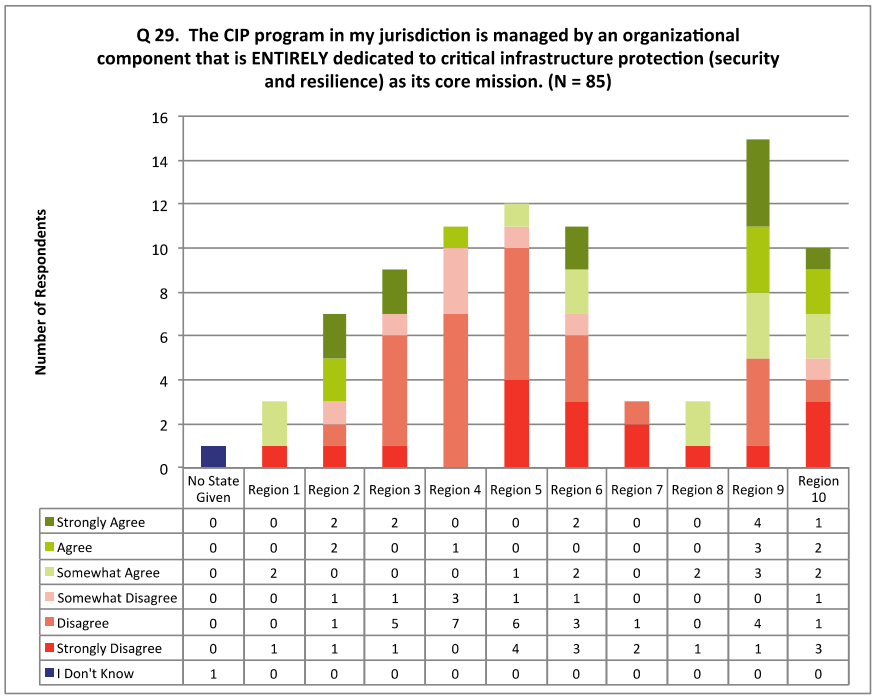
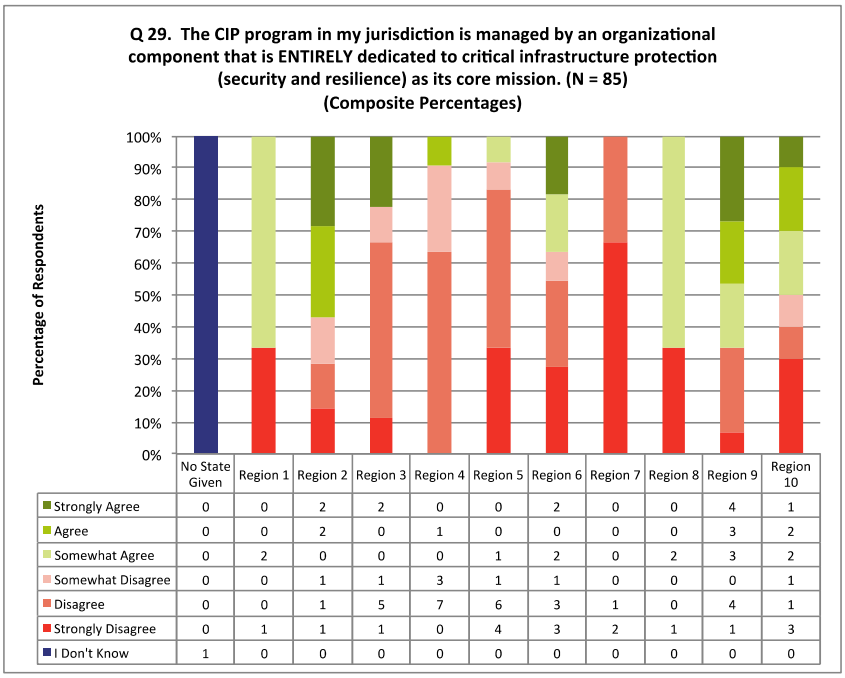


Figure 20D. Composite percentages of Figure 20C.



	No State Given	Region 1	Region 2	Region 3	Region 4	Region 5	Region 6	Region 7	Region 8	Region 9	Region 10
Strongly Agree	0	0	2	2	0	0	2	0	0	4	1
Agree	0	0	2	0	1	0	0	0	0	3	2
Somewhat Agree	0	2	0	0	0	1	2	0	2	3	2
Somewhat Disagree	0	0	1	1	3	1	1	0	0	0	1
Disagree	0	0	1	5	7	6	3	1	0	4	1
Strongly Disagree	0	1	1	1	0	4	3	2	1	1	3
I Don't Know	1	0	0	0	0	0	0	0	0	0	0

Figure 20E. Figure 20 cross-analyzed by respondents federal FEMA region.



	No State Given	Region 1	Region 2	Region 3	Region 4	Region 5	Region 6	Region 7	Region 8	Region 9	Region 10
Strongly Agree	0	0	2	2	0	0	2	0	0	4	1
Agree	0	0	2	0	1	0	0	0	0	3	2
Somewhat Agree	0	2	0	0	0	1	2	0	2	3	2
Somewhat Disagree	0	0	1	1	3	1	1	0	0	0	1
Disagree	0	0	1	5	7	6	3	1	0	4	1
Strongly Disagree	0	1	1	1	0	4	3	2	1	1	3
I Don't Know	1	0	0	0	0	0	0	0	0	0	0

Figure 20F. Composite percentages of Figure 20F.

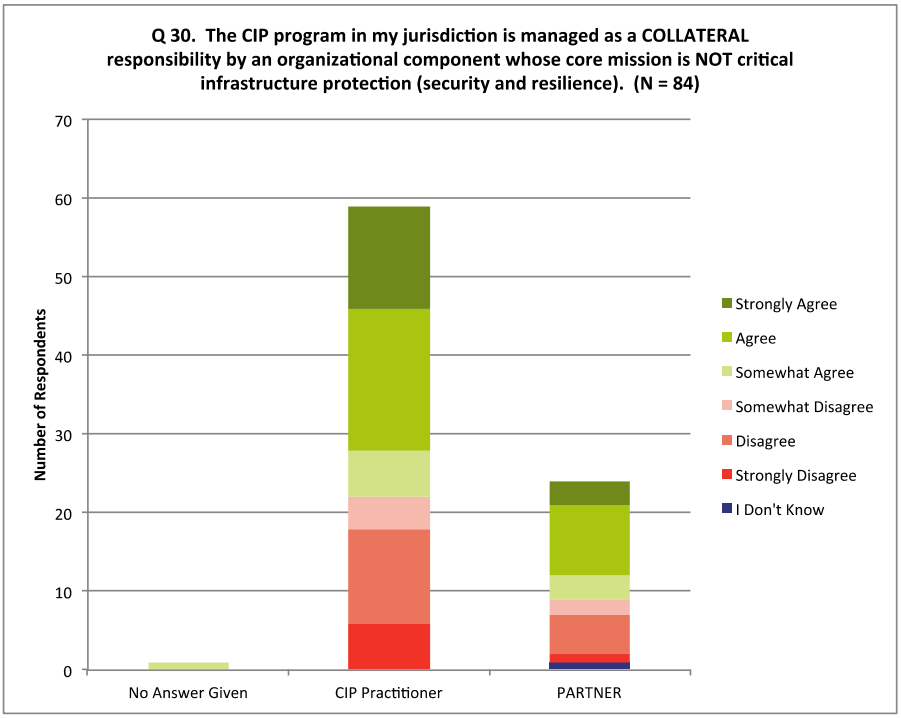


Figure 21A. Figure 21 cross-analyzed by respondents that self-identify as a CIP practitioner or partner.

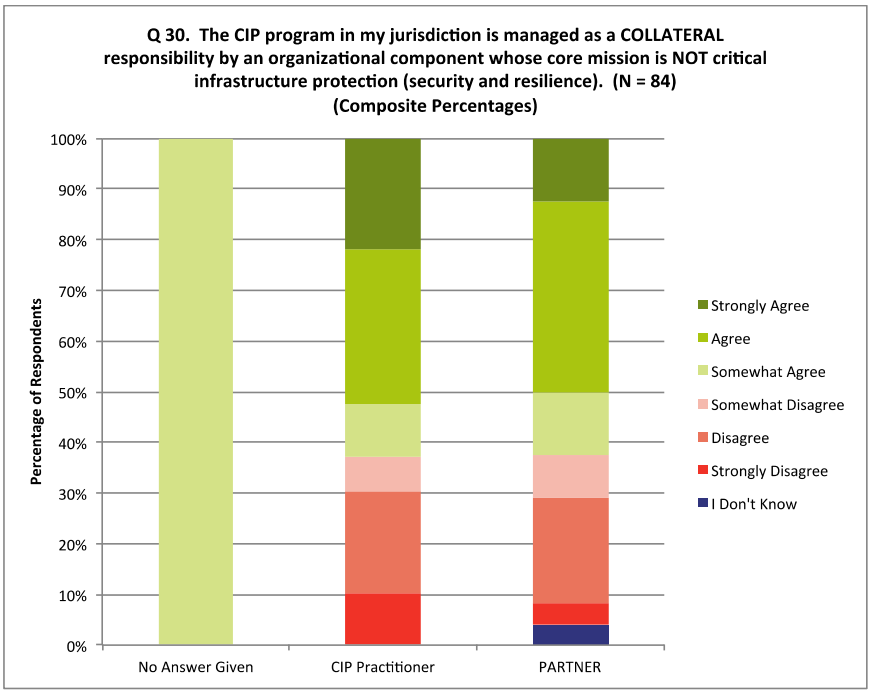


Figure 21B. Composite percentages of Figure 21A.

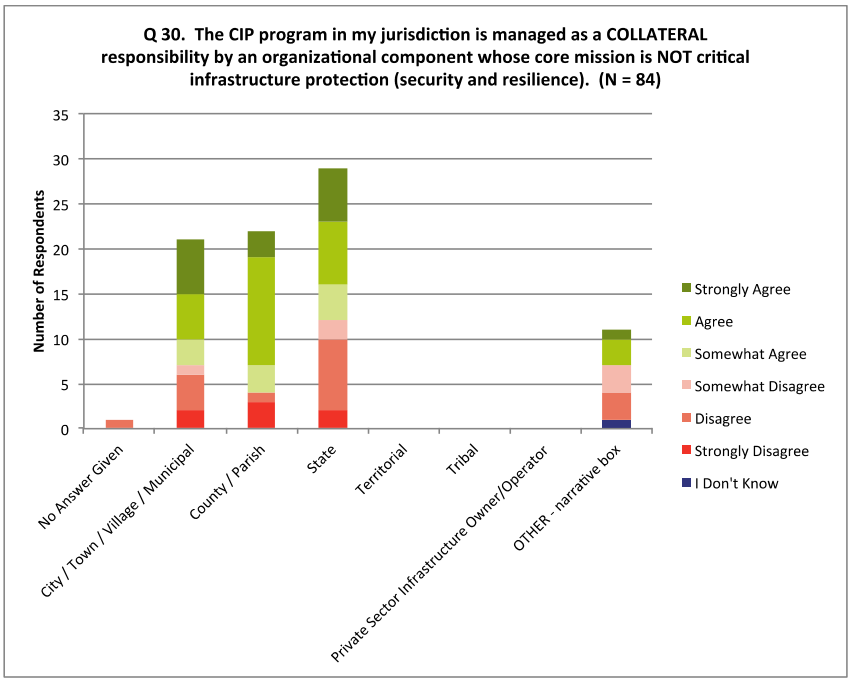


Figure 21C. Figure 21 cross-analyzed by respondents jurisdiction type.

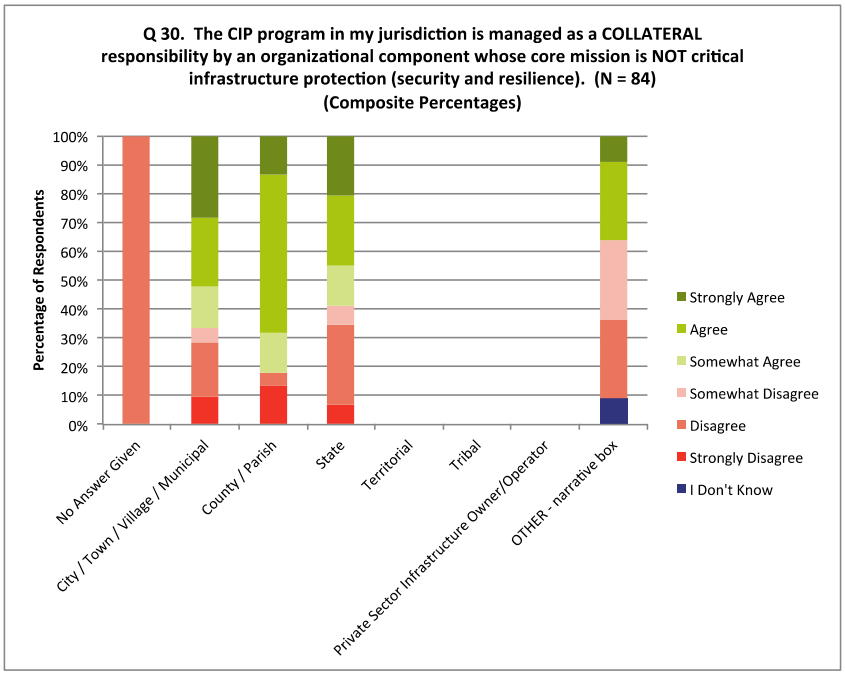
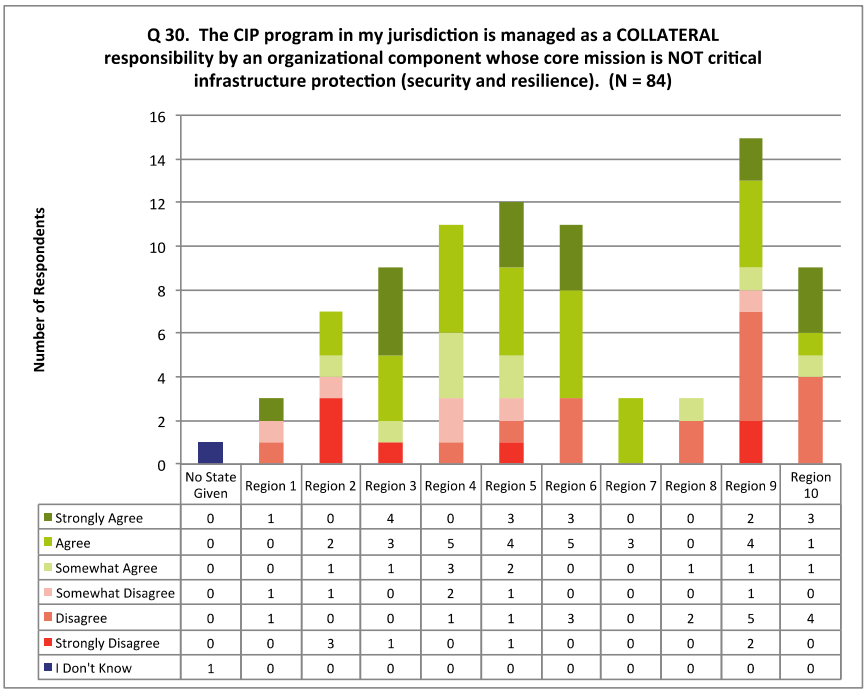
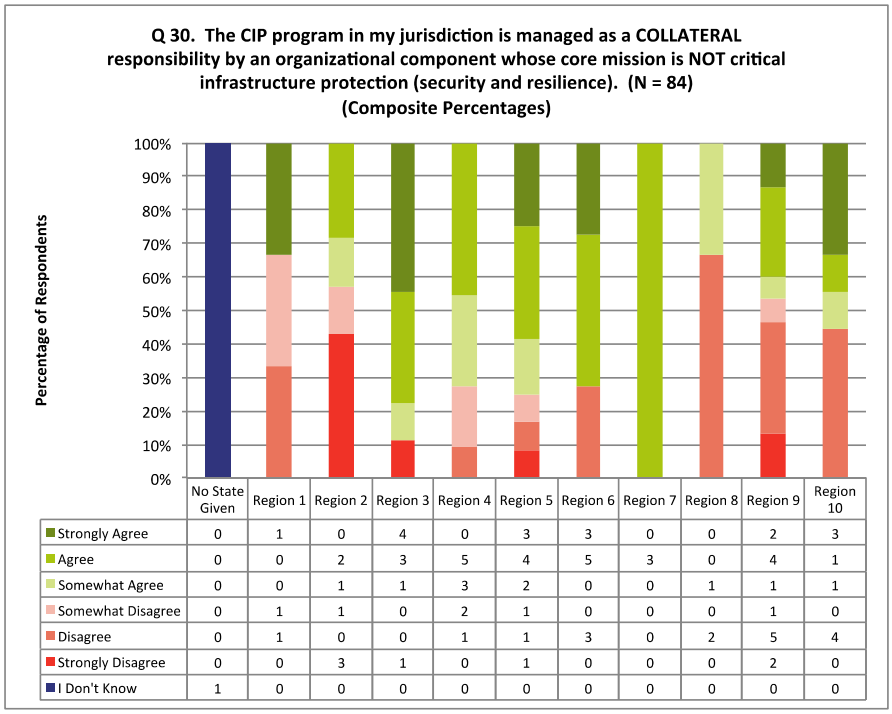


Figure 21D. Composite percentages of Figure 21C.



	No State Given	Region 1	Region 2	Region 3	Region 4	Region 5	Region 6	Region 7	Region 8	Region 9	Region 10
Strongly Agree	0	1	0	4	0	3	3	0	0	2	3
Agree	0	0	2	3	5	4	5	3	0	4	1
Somewhat Agree	0	0	1	1	3	2	0	0	1	1	1
Somewhat Disagree	0	1	1	0	2	1	0	0	0	1	0
Disagree	0	1	0	0	1	1	3	0	2	5	4
Strongly Disagree	0	0	3	1	0	1	0	0	0	2	0
I Don't Know	1	0	0	0	0	0	0	0	0	0	0

Figure 21E. Figure 21 cross-analyzed by respondents federal FEMA region.



	No State Given	Region 1	Region 2	Region 3	Region 4	Region 5	Region 6	Region 7	Region 8	Region 9	Region 10
Strongly Agree	0	1	0	4	0	3	3	0	0	2	3
Agree	0	0	2	3	5	4	5	3	0	4	1
Somewhat Agree	0	0	1	1	3	2	0	0	1	1	1
Somewhat Disagree	0	1	1	0	2	1	0	0	0	1	0
Disagree	0	1	0	0	1	1	3	0	2	5	4
Strongly Disagree	0	0	3	1	0	1	0	0	0	2	0
I Don't Know	1	0	0	0	0	0	0	0	0	0	0

Figure 21F. Composite percentages of Figure 22A.

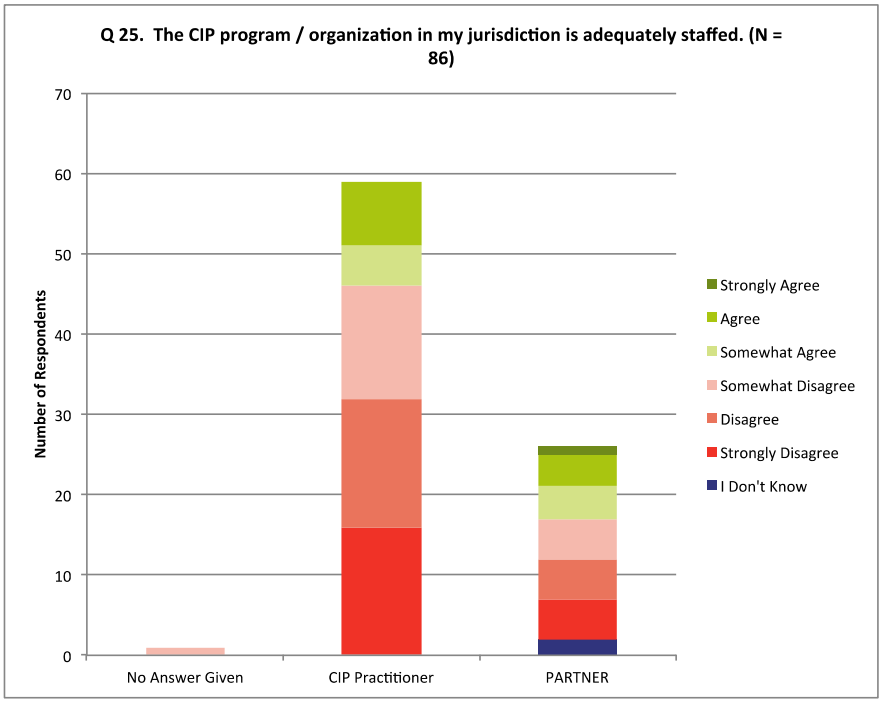


Figure 22A. Figure 22 cross-analyzed by respondents that self-identify as a CIP practitioner or partner.

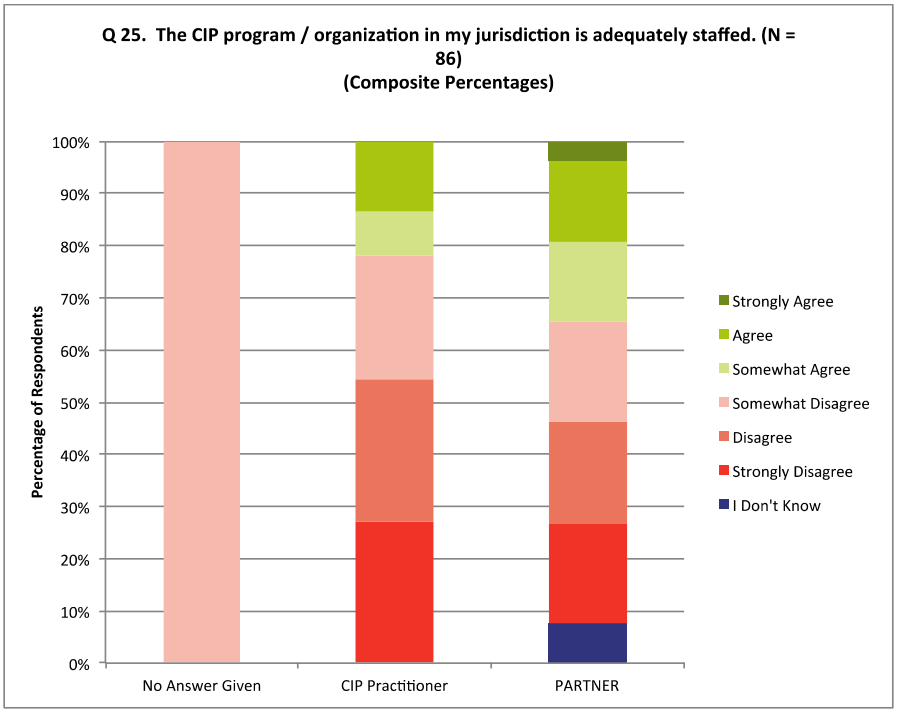


Figure 22B. Composite percentages of Figure 22A.

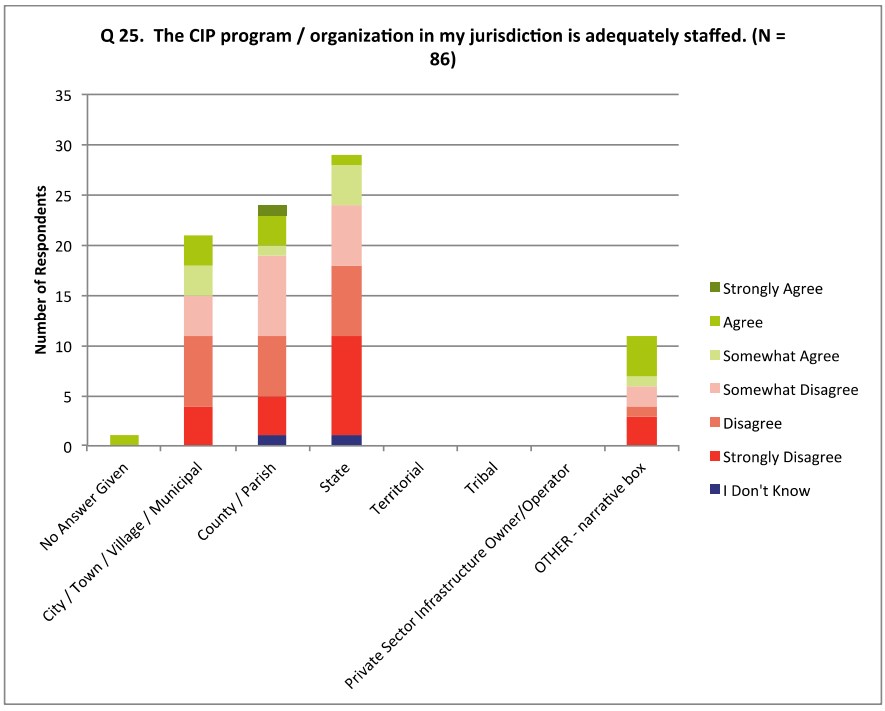


Figure 22C. Figure 22 cross-analyzed by respondents jurisdiction type.

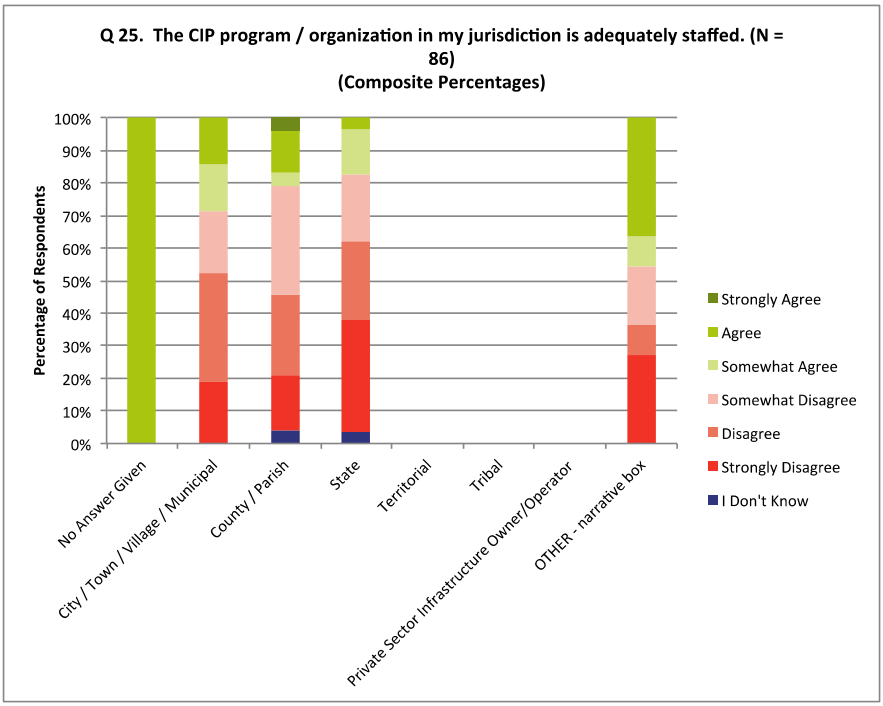
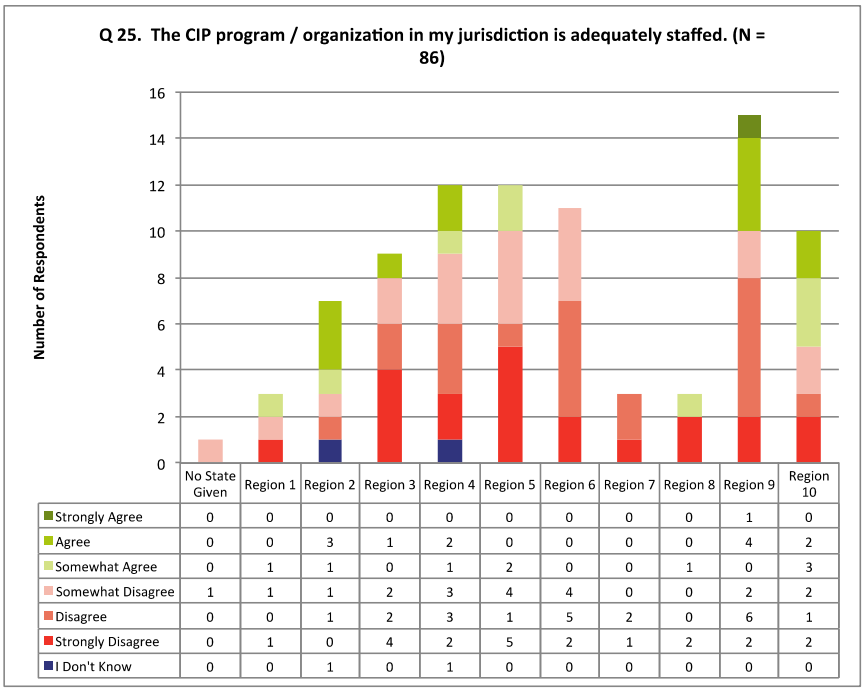
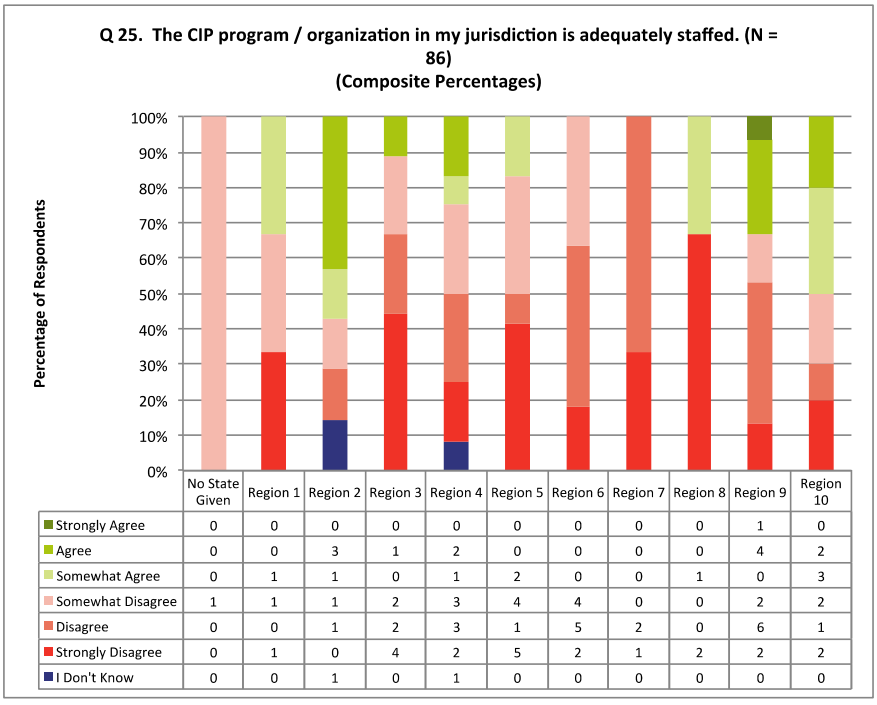


Figure 22D. Composite percentages of Figure 22C.



	No State Given	Region 1	Region 2	Region 3	Region 4	Region 5	Region 6	Region 7	Region 8	Region 9	Region 10
Strongly Agree	0	0	0	0	0	0	0	0	0	1	0
Agree	0	0	3	1	2	0	0	0	0	4	2
Somewhat Agree	0	1	1	0	1	2	0	0	1	0	3
Somewhat Disagree	1	1	1	2	3	4	4	0	0	2	2
Disagree	0	0	1	2	3	1	5	2	0	6	1
Strongly Disagree	0	1	0	4	2	5	2	1	2	2	2
I Don't Know	0	0	1	0	1	0	0	0	0	0	0

Figure 22E. Figure 22 cross-analyzed by respondents federal FEMA region.



	No State Given	Region 1	Region 2	Region 3	Region 4	Region 5	Region 6	Region 7	Region 8	Region 9	Region 10
Strongly Agree	0	0	0	0	0	0	0	0	0	1	0
Agree	0	0	3	1	2	0	0	0	0	4	2
Somewhat Agree	0	1	1	0	1	2	0	0	1	0	3
Somewhat Disagree	1	1	1	2	3	4	4	0	0	2	2
Disagree	0	0	1	2	3	1	5	2	0	6	1
Strongly Disagree	0	1	0	4	2	5	2	1	2	2	2
I Don't Know	0	0	1	0	1	0	0	0	0	0	0

Figure 22F. Composite percentages of Figure 22E.

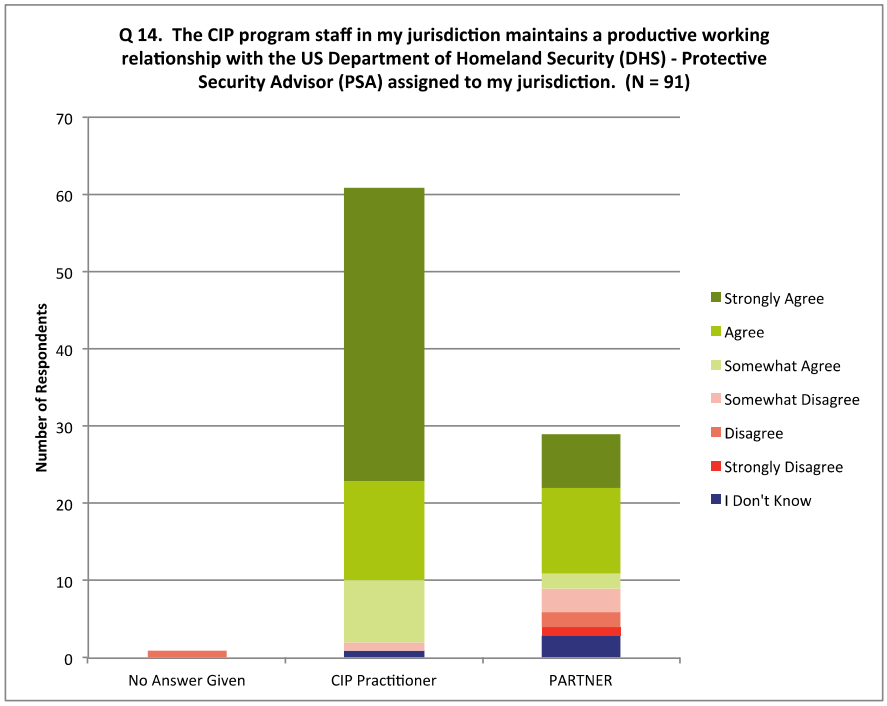


Figure 26A. Figure 26 cross-analyzed by respondents that self-identify as a CIP practitioner or partner.

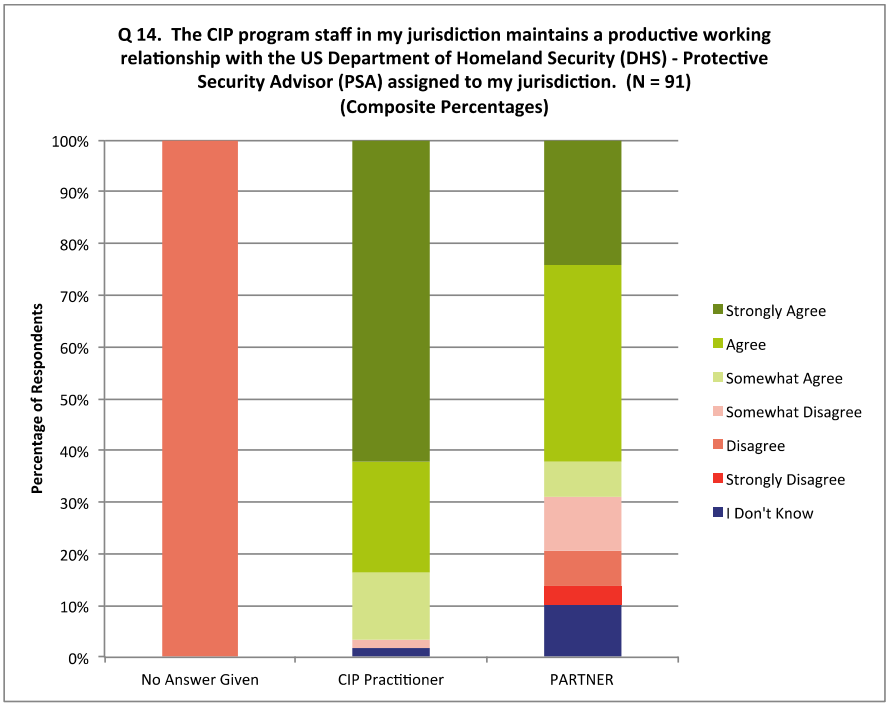


Figure 26B. Composite percentages of Figure 26A.

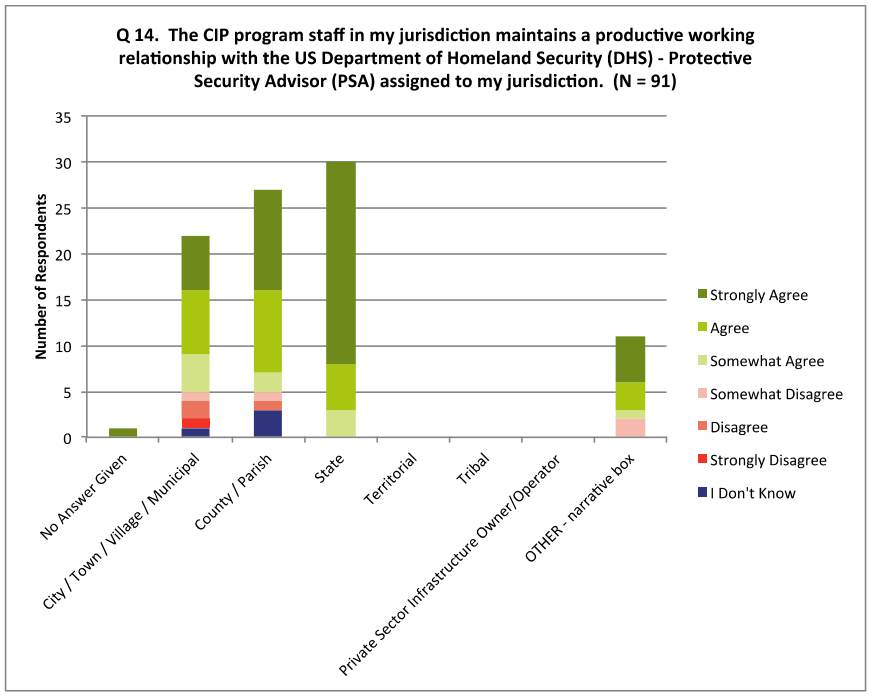


Figure 26C. Figure 26 cross-analyzed by respondents jurisdiction type.

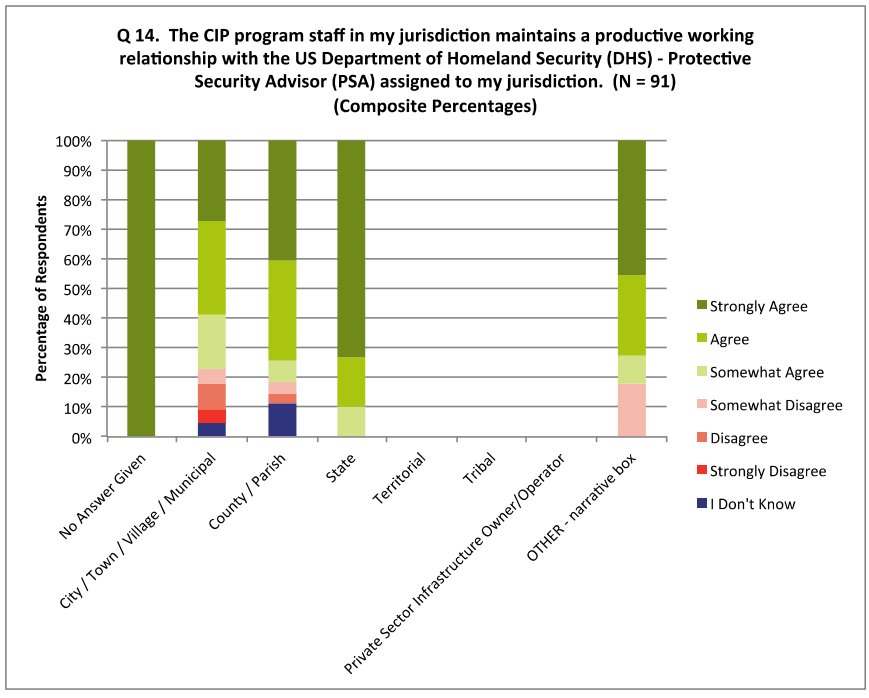
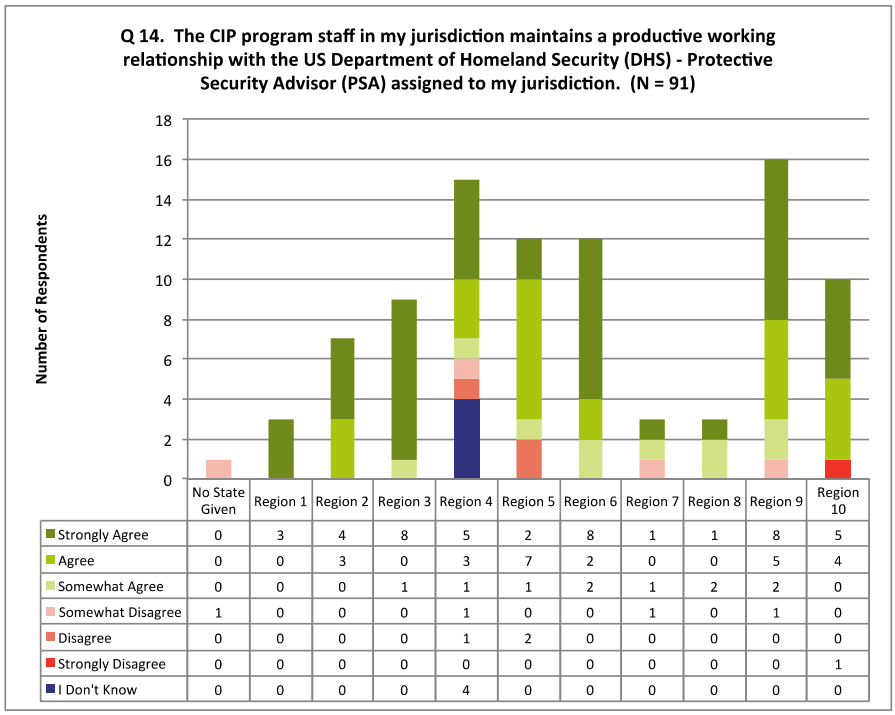
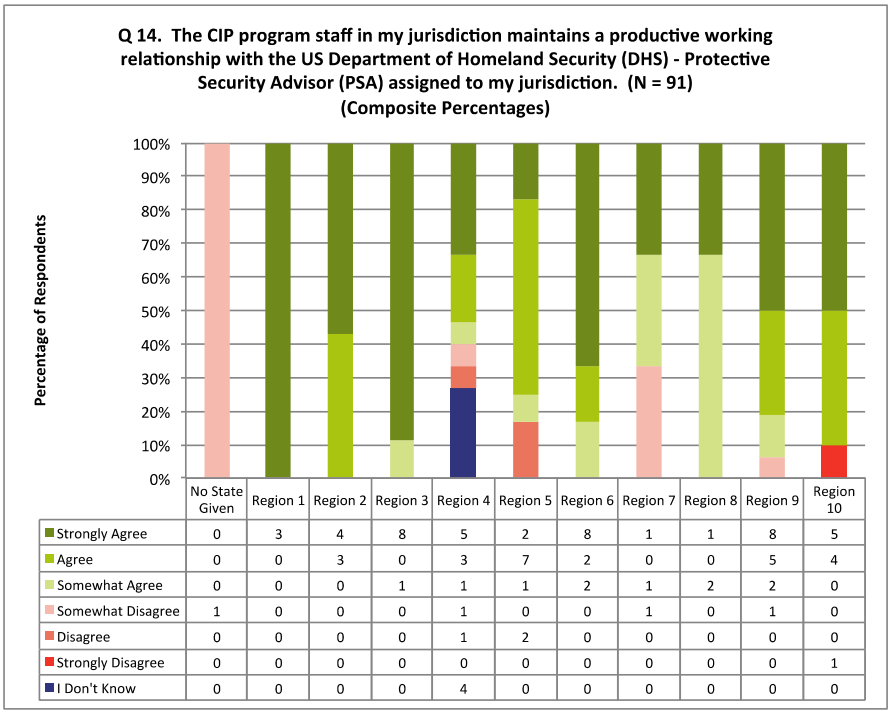


Figure 26D. Composite percentages of Figure 26C.



	No State Given	Region 1	Region 2	Region 3	Region 4	Region 5	Region 6	Region 7	Region 8	Region 9	Region 10
Strongly Agree	0	3	4	8	5	2	8	1	1	8	5
Agree	0	0	3	0	3	7	2	0	0	5	4
Somewhat Agree	0	0	0	1	1	1	2	1	2	2	0
Somewhat Disagree	1	0	0	0	1	0	0	1	0	1	0
Disagree	0	0	0	0	1	2	0	0	0	0	0
Strongly Disagree	0	0	0	0	0	0	0	0	0	0	1
I Don't Know	0	0	0	0	4	0	0	0	0	0	0

Figure 26E. Figure 26 cross-analyzed by respondents federal FEMA region.



	No State Given	Region 1	Region 2	Region 3	Region 4	Region 5	Region 6	Region 7	Region 8	Region 9	Region 10
Strongly Agree	0	3	4	8	5	2	8	1	1	8	5
Agree	0	0	3	0	3	7	2	0	0	5	4
Somewhat Agree	0	0	0	1	1	1	2	1	2	2	0
Somewhat Disagree	1	0	0	0	1	0	0	1	0	1	0
Disagree	0	0	0	0	1	2	0	0	0	0	0
Strongly Disagree	0	0	0	0	0	0	0	0	0	0	1
I Don't Know	0	0	0	0	4	0	0	0	0	0	0

Figure 26F. Composite percentages of Figure 26E.

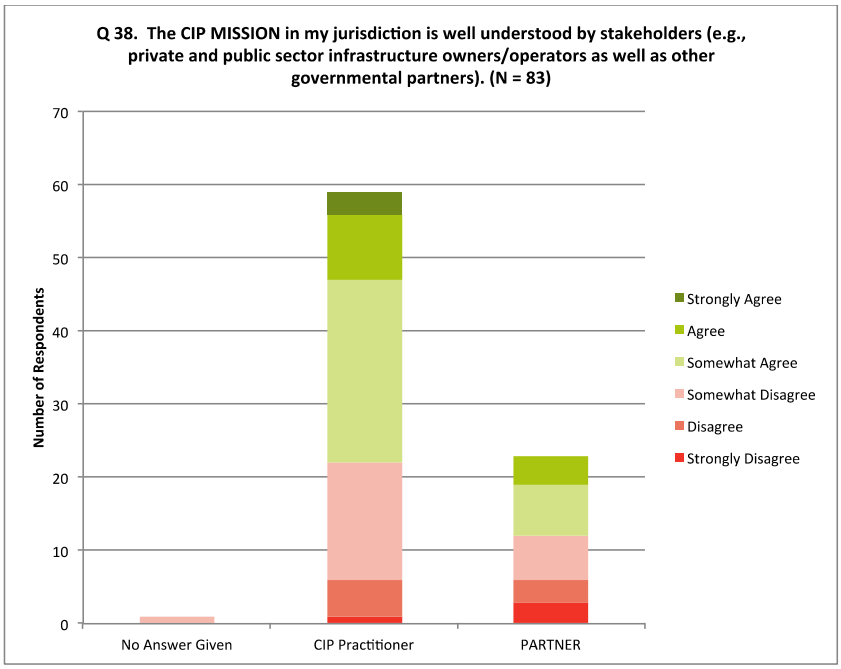


Figure 27A. Figure 27 cross-analyzed by respondents that self-identify as a CIP practitioner or partner.

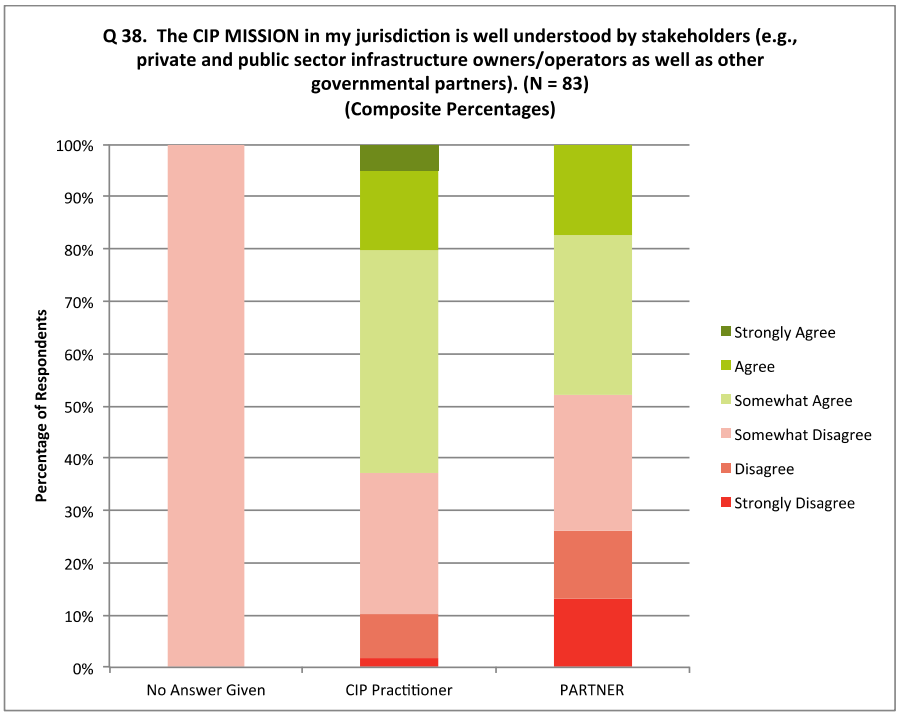


Figure 27B. Composite percentages of Figure 27A.

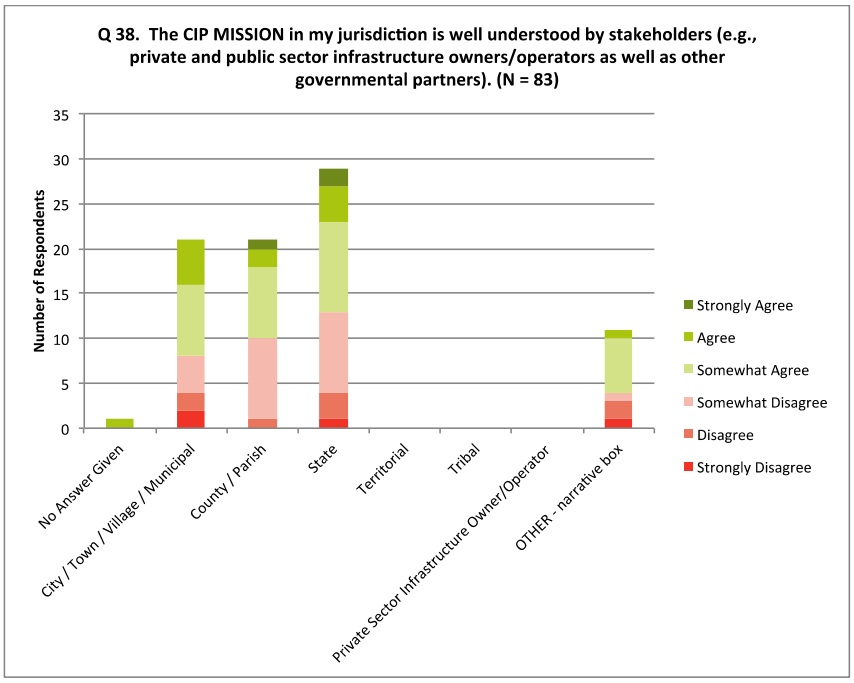


Figure 27C. Figure 27 cross-analyzed by respondents jurisdiction type.

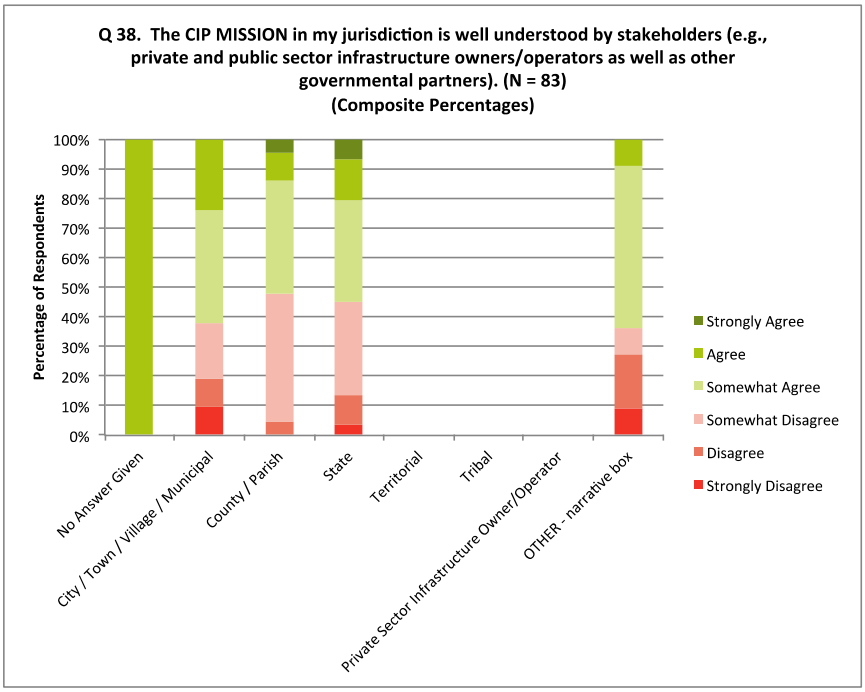
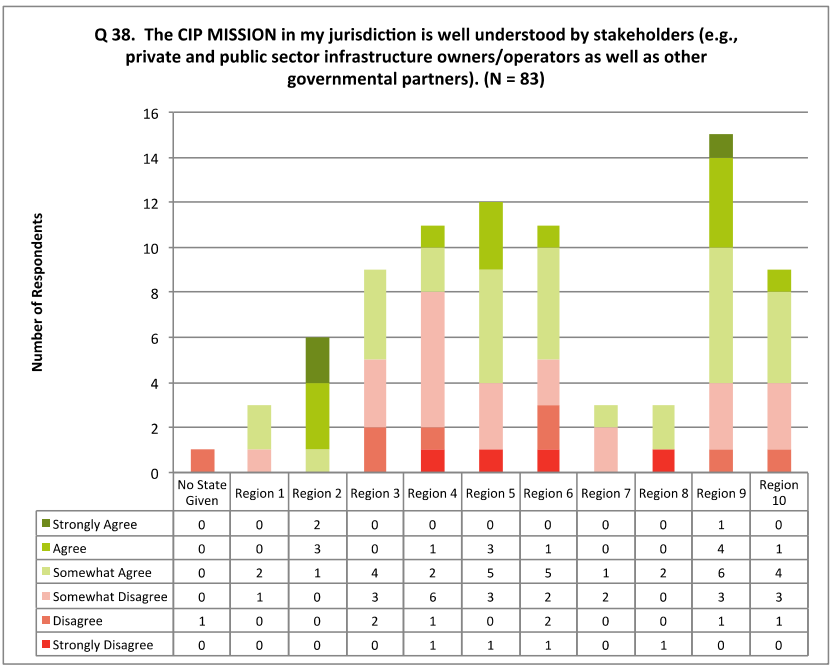
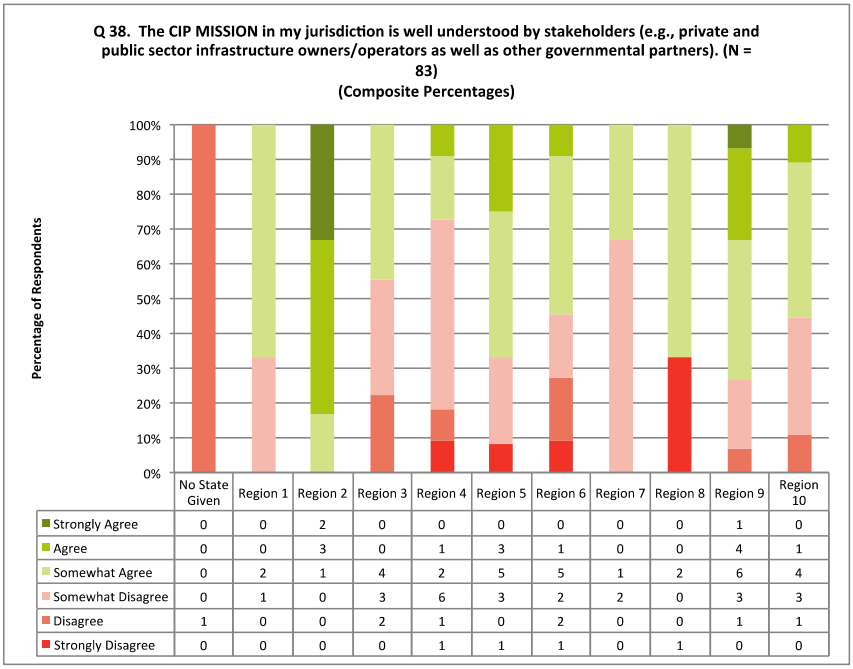


Figure 27D. Composite percentages of Figure 27C.



	No State Given	Region 1	Region 2	Region 3	Region 4	Region 5	Region 6	Region 7	Region 8	Region 9	Region 10
Strongly Agree	0	0	2	0	0	0	0	0	0	1	0
Agree	0	0	3	0	1	3	1	0	0	4	1
Somewhat Agree	0	2	1	4	2	5	5	1	2	6	4
Somewhat Disagree	0	1	0	3	6	3	2	2	0	3	3
Disagree	1	0	0	2	1	0	2	0	0	1	1
Strongly Disagree	0	0	0	0	1	1	1	0	1	0	0

Figure 27E. Figure 27 cross-analyzed by respondents federal FEMA region.



	No State Given	Region 1	Region 2	Region 3	Region 4	Region 5	Region 6	Region 7	Region 8	Region 9	Region 10
Strongly Agree	0	0	2	0	0	0	0	0	0	1	0
Agree	0	0	3	0	1	3	1	0	0	4	1
Somewhat Agree	0	2	1	4	2	5	5	1	2	6	4
Somewhat Disagree	0	1	0	3	6	3	2	2	0	3	3
Disagree	1	0	0	2	1	0	2	0	0	1	1
Strongly Disagree	0	0	0	0	1	1	1	0	1	0	0

Figure 27F. Composite percentages of Figure 27E.

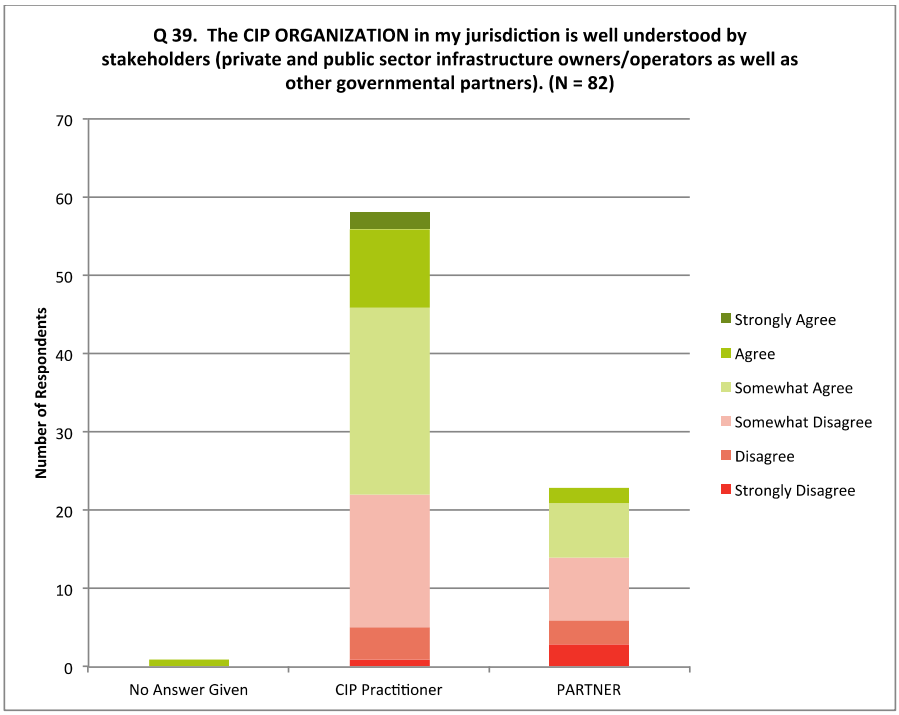


Figure 28A. Figure 28 cross-analyzed by respondents that self-identify as a CIP practitioner or partner.

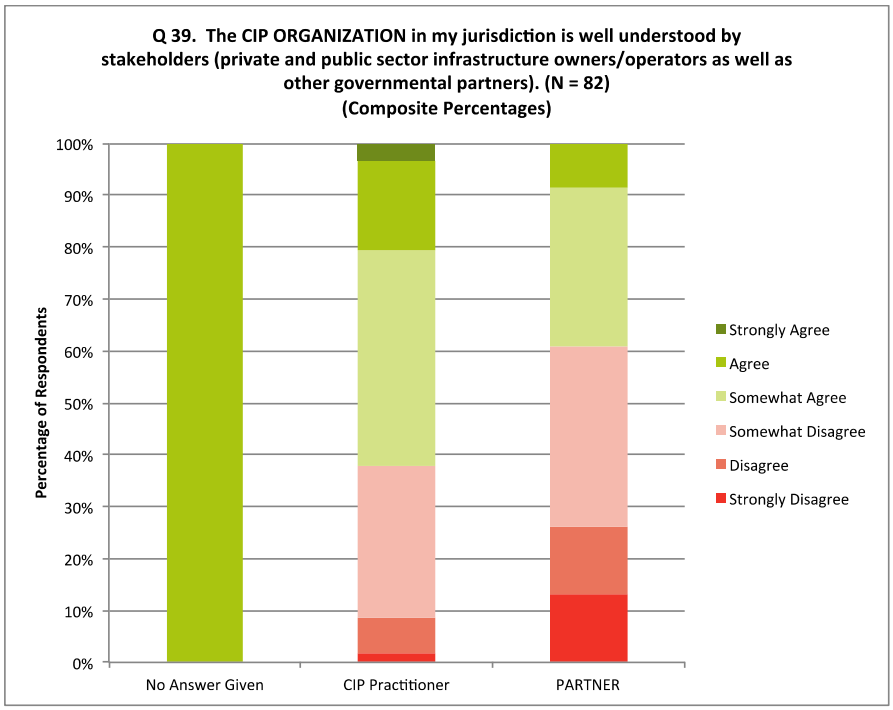


Figure 28B. Composite percentages of Figure 28A.

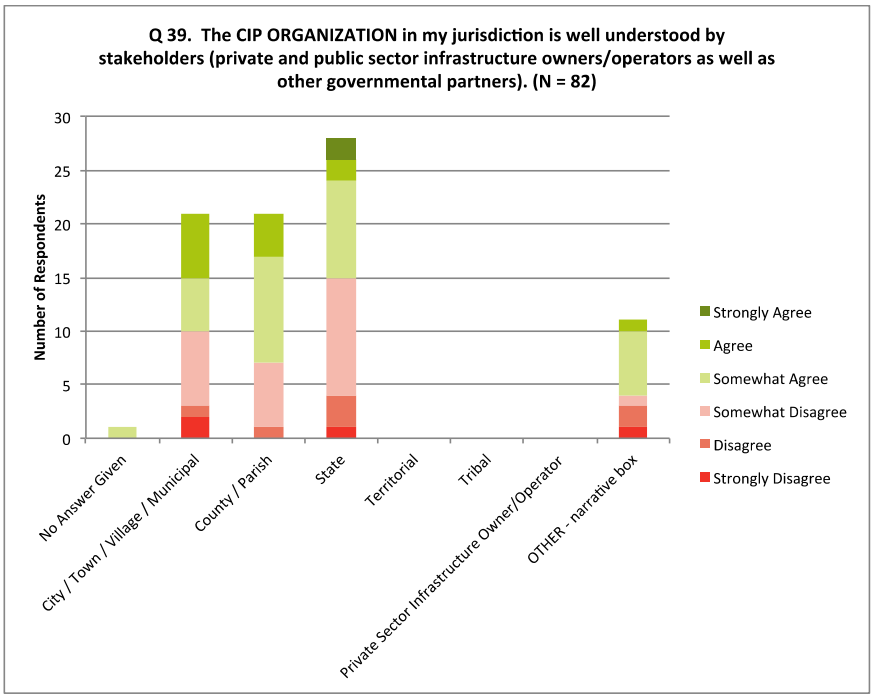


Figure 28C. Figure 28 cross-analyzed by respondents jurisdiction type.

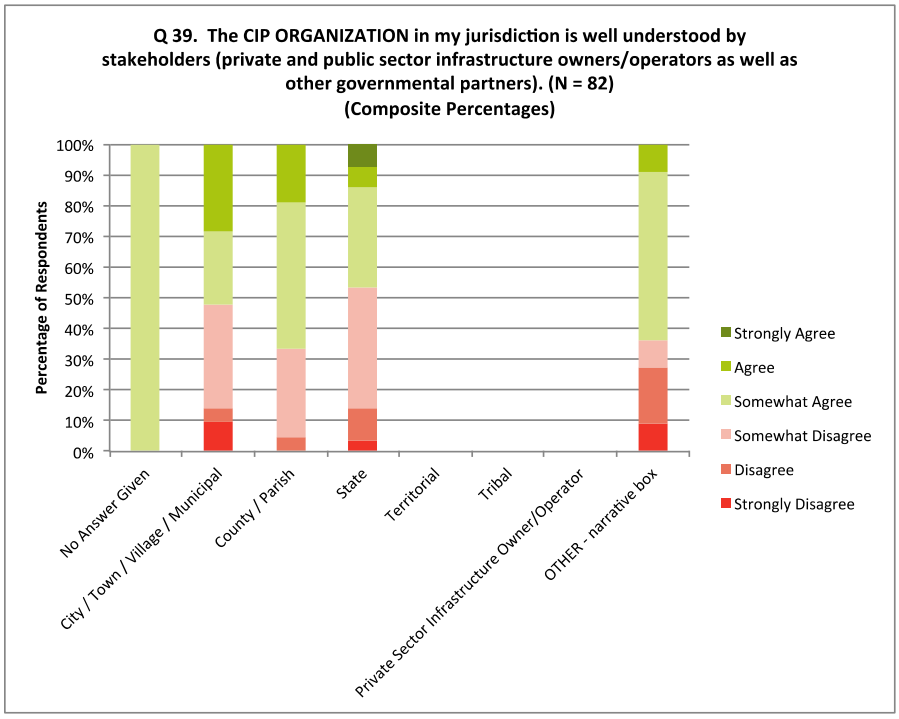
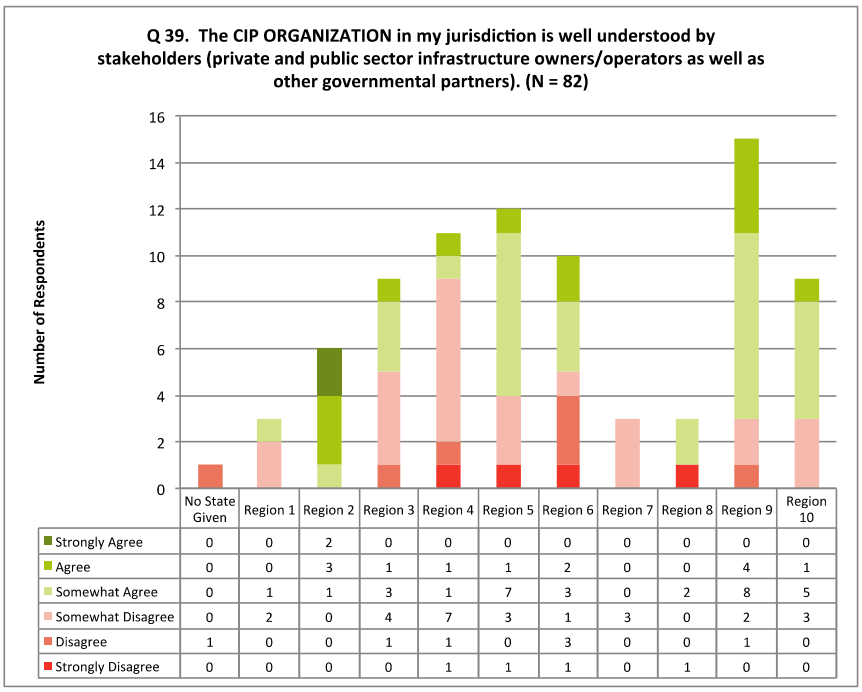
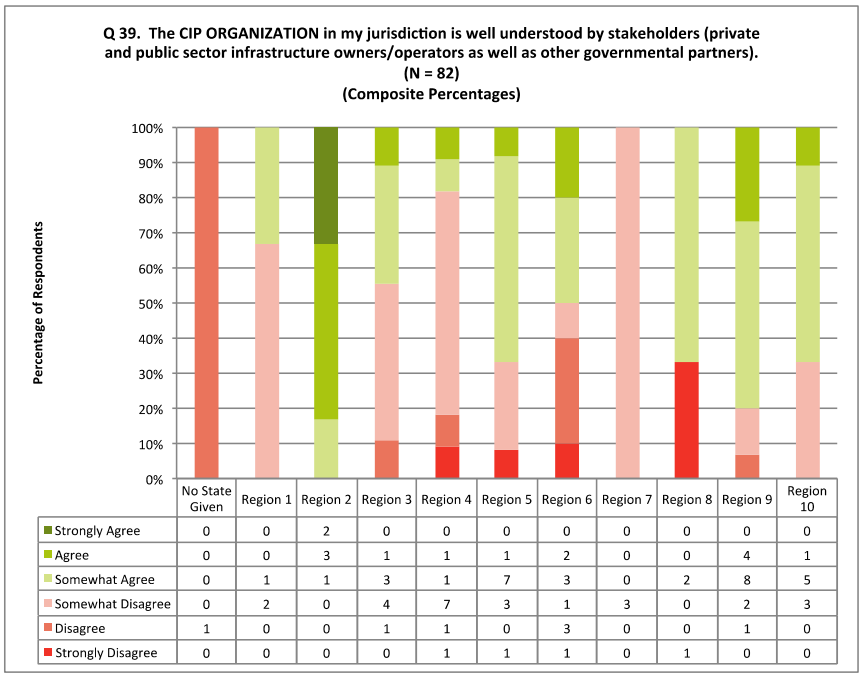


Figure 28D. Composite percentages of Figure 28C.



	No State Given	Region 1	Region 2	Region 3	Region 4	Region 5	Region 6	Region 7	Region 8	Region 9	Region 10
Strongly Agree	0	0	2	0	0	0	0	0	0	0	0
Agree	0	0	3	1	1	1	2	0	0	4	1
Somewhat Agree	0	1	1	3	1	7	3	0	2	8	5
Somewhat Disagree	0	2	0	4	7	3	1	3	0	2	3
Disagree	1	0	0	1	1	0	3	0	0	1	0
Strongly Disagree	0	0	0	0	1	1	1	0	1	0	0

Figure 28E. Figure 28 cross-analyzed by respondents federal FEMA region.



	No State Given	Region 1	Region 2	Region 3	Region 4	Region 5	Region 6	Region 7	Region 8	Region 9	Region 10
Strongly Agree	0	0	2	0	0	0	0	0	0	0	0
Agree	0	0	3	1	1	1	2	0	0	4	1
Somewhat Agree	0	1	1	3	1	7	3	0	2	8	5
Somewhat Disagree	0	2	0	4	7	3	1	3	0	2	3
Disagree	1	0	0	1	1	0	3	0	0	1	0
Strongly Disagree	0	0	0	0	1	1	1	0	1	0	0

Figure 28F. Composite percentages of Figure 28E.

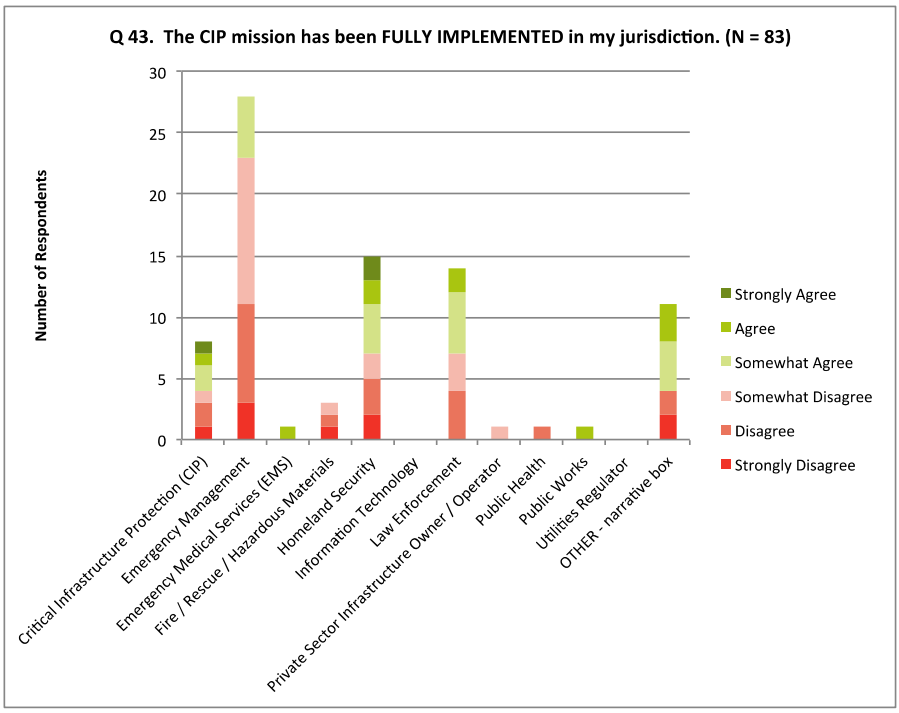


Figure 29A. Figure 29 cross-analyzed by respondents organization type.

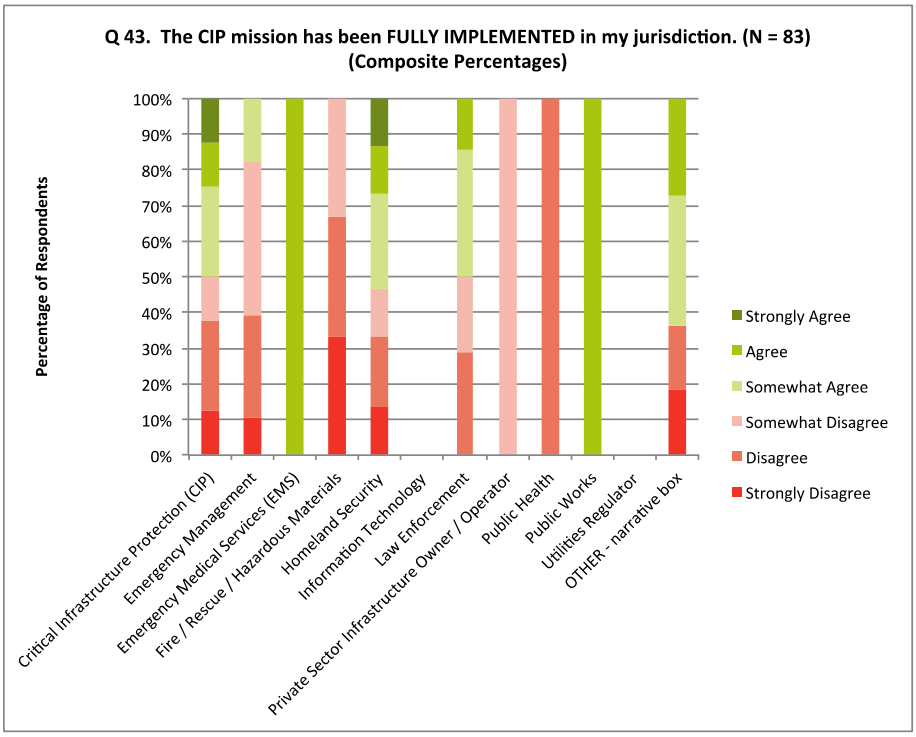


Figure 29B. Composite percentages of Figure 29A.

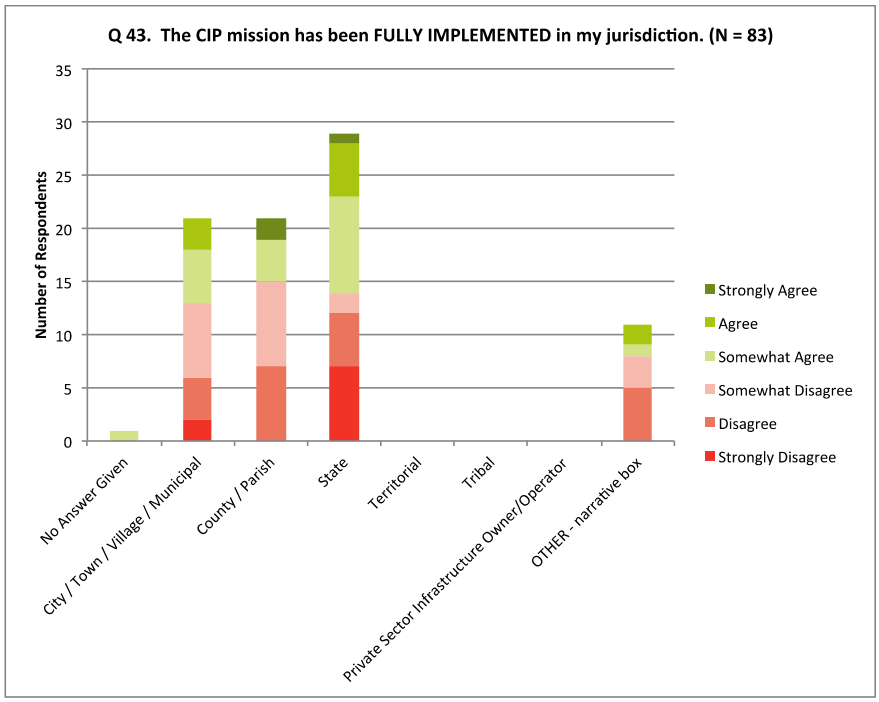


Figure 29C. Figure 29 cross-analyzed by respondents jurisdiction type.

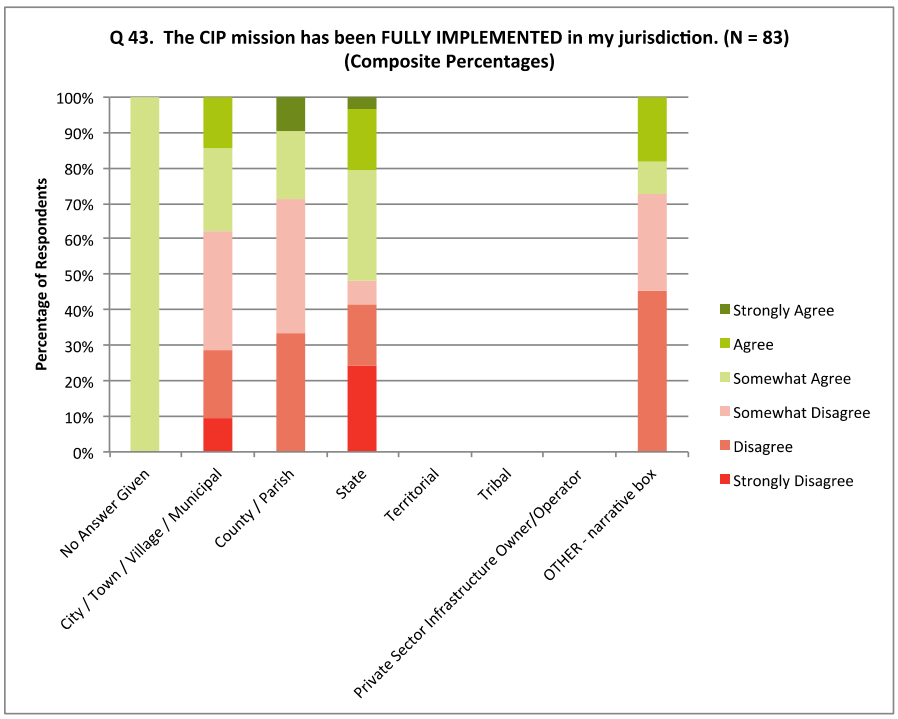


Figure 29D. Composite percentages of Figure 29C.

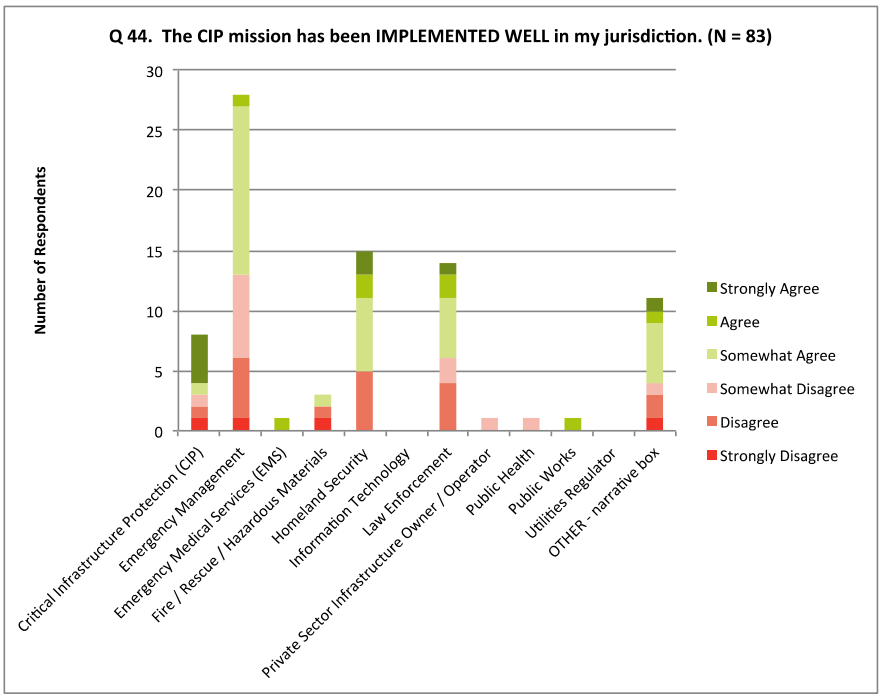


Figure 30A Figure 30 cross-analyzed by respondents organization type.

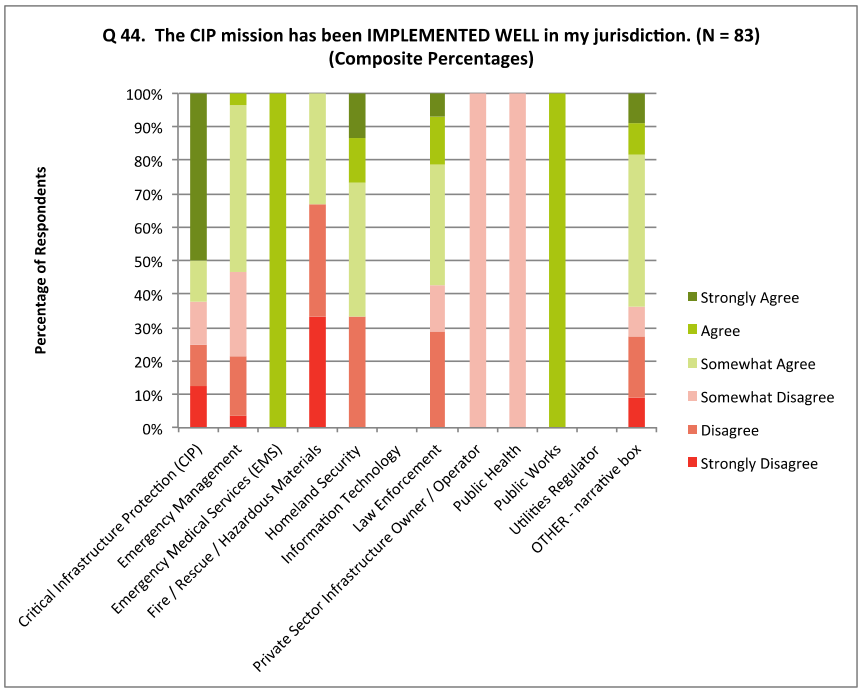


Figure 30B. Composite percentages of Figure 30A.

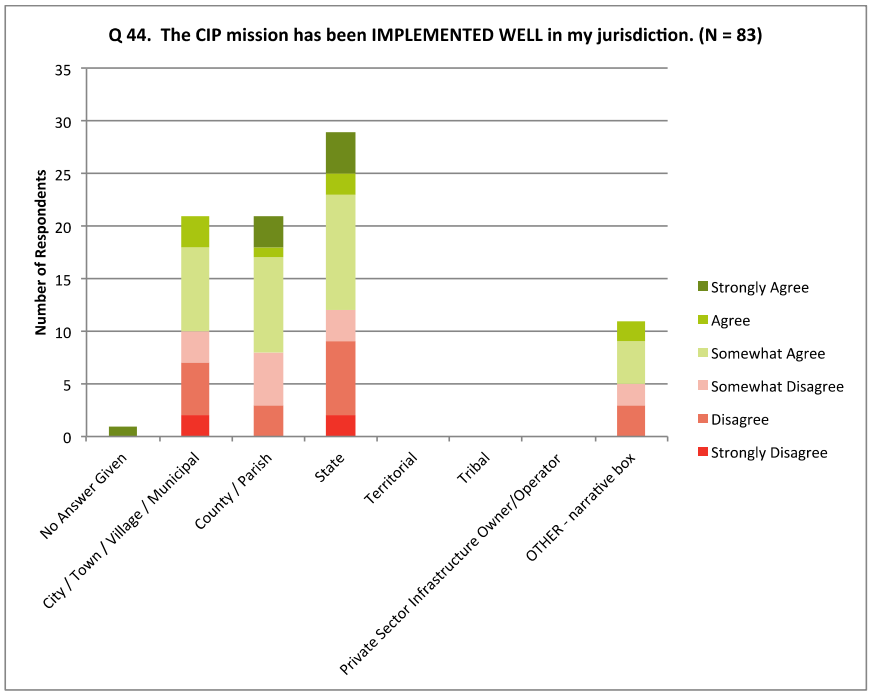


Figure 30C. Figure 30 cross-analyzed by respondents jurisdiction type.

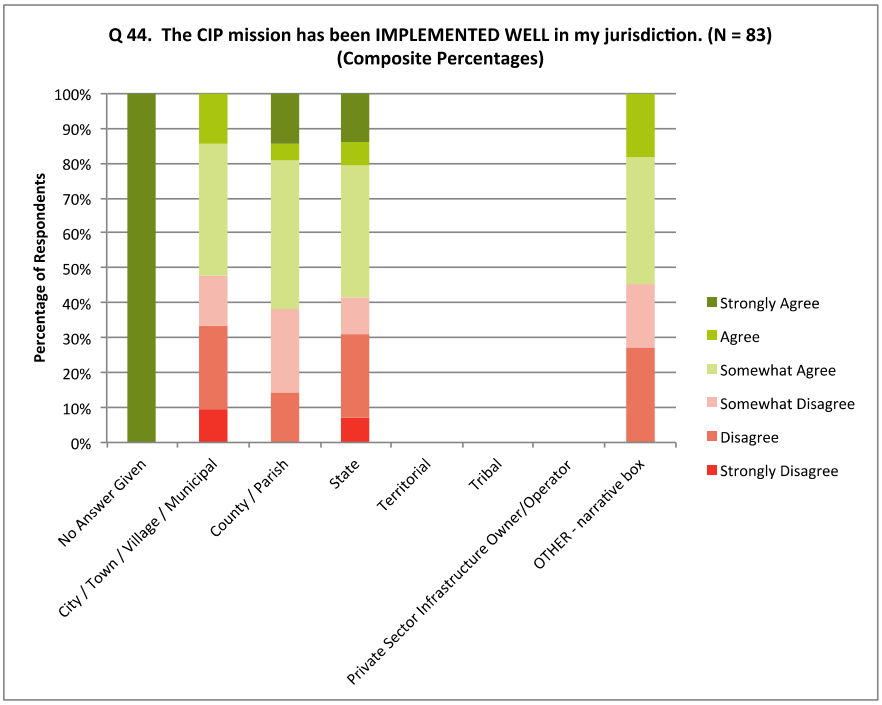


Figure 30D. Composite percentages of Figure 30C.

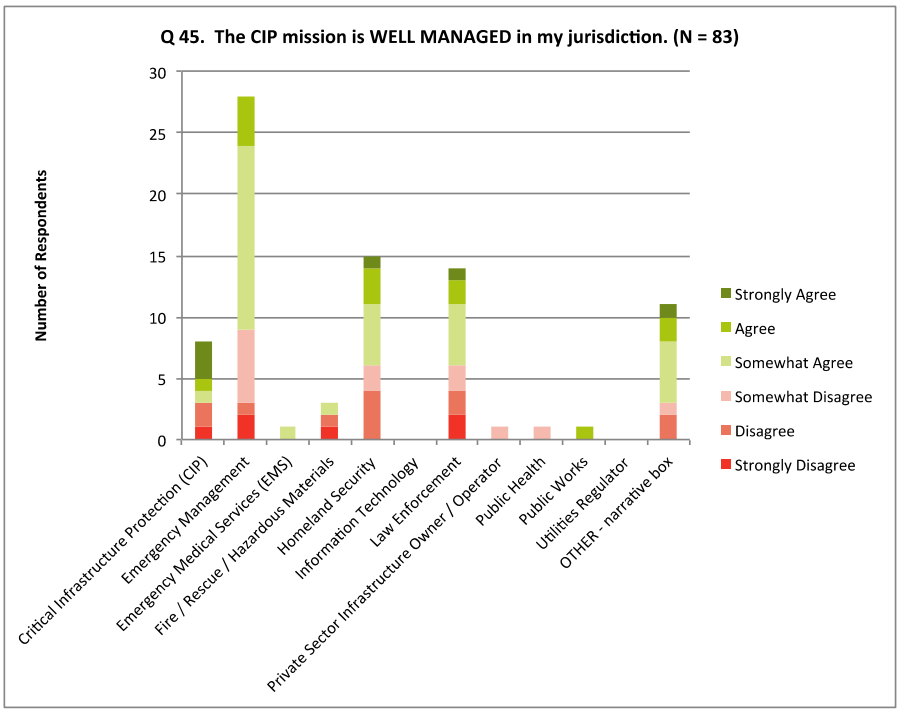


Figure 31A. Figure 31 cross-analyzed by respondents organization type.

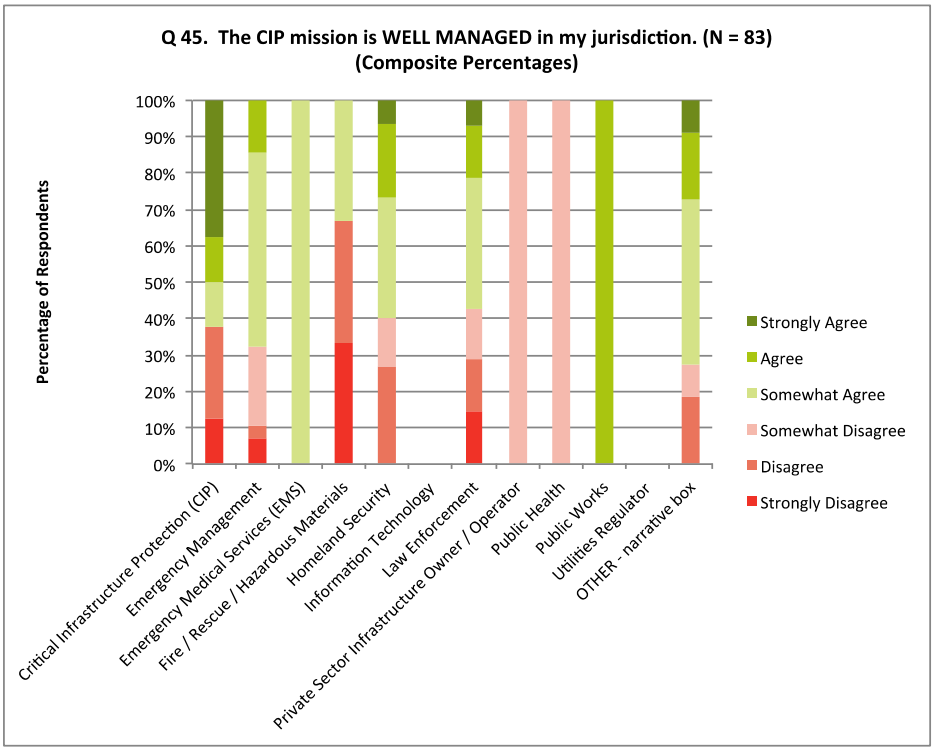


Figure 31B. Composite percentages of Figure 31A.

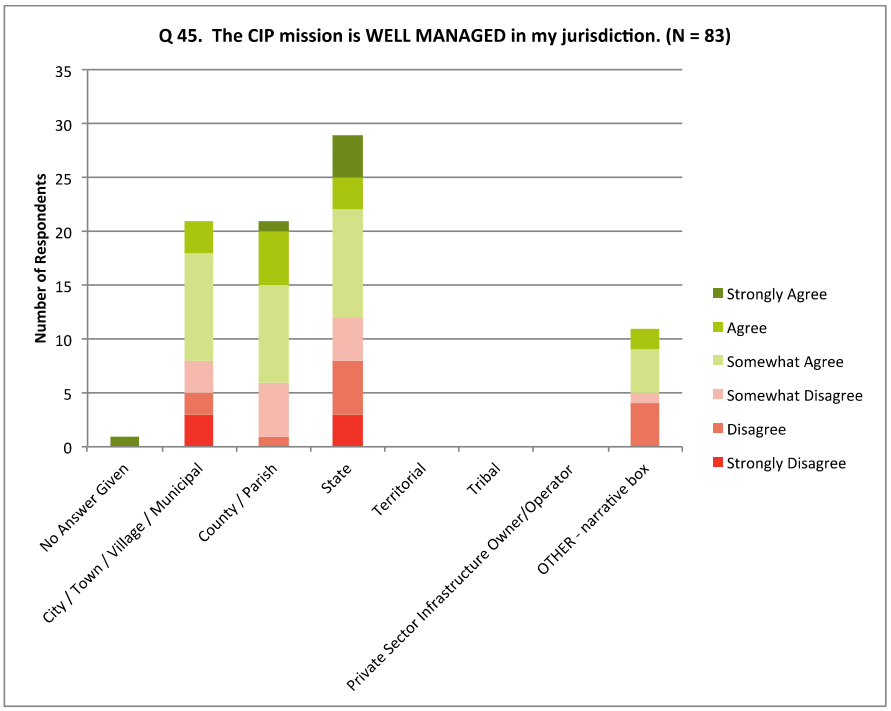


Figure 31C. Figure 31 cross-analyzed by respondents jurisdiction type.

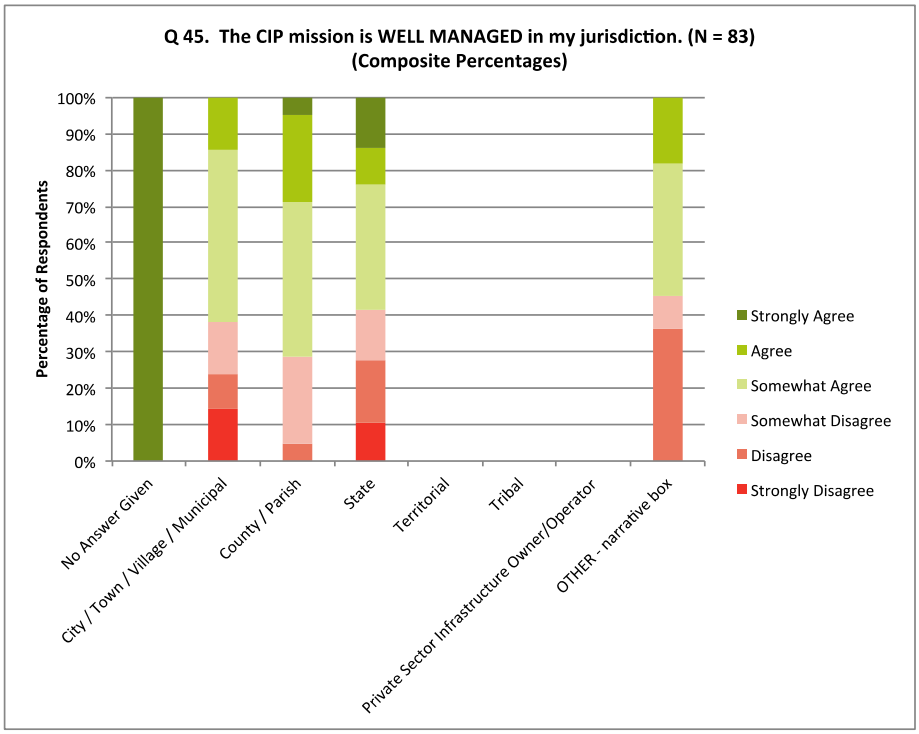


Figure 31D. Composite percentages of Figure 31C.

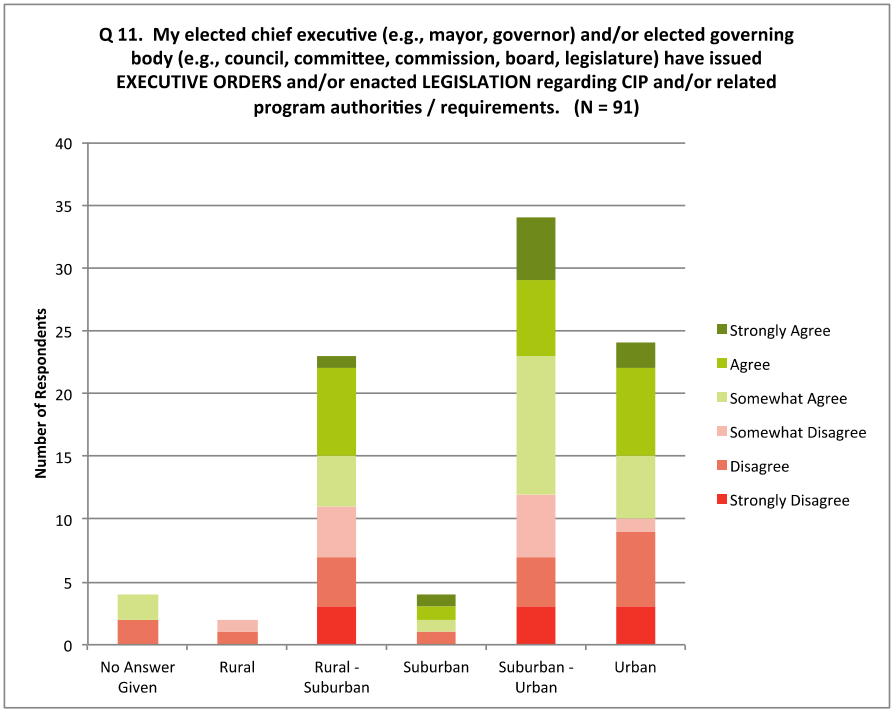


Figure 32A. Figure 32 cross-analyzed by respondents jurisdiction type.

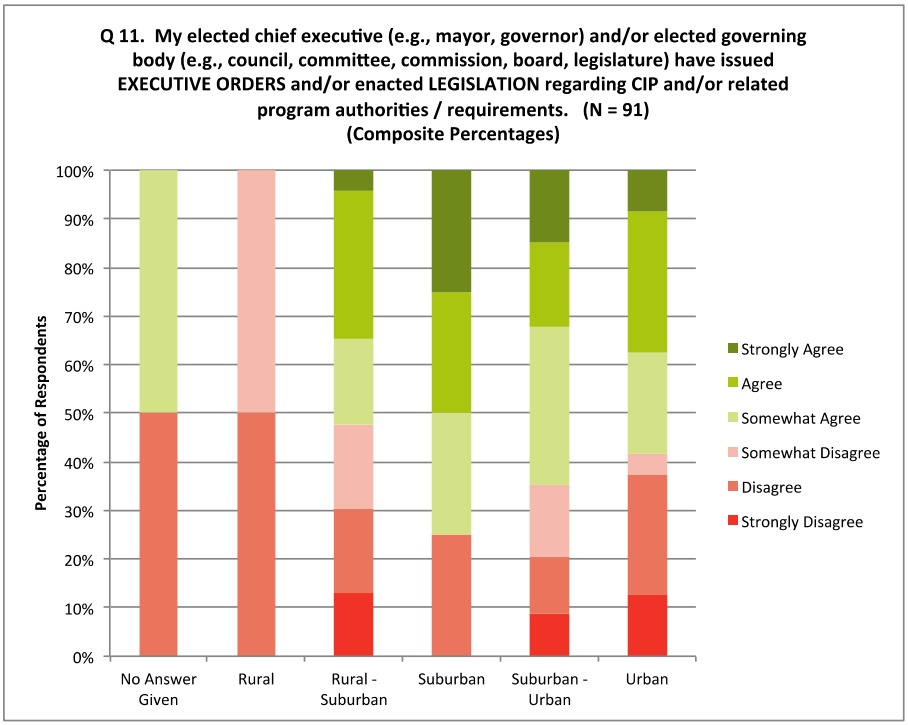


Figure 32B. Composite percentages of Figure 32A.

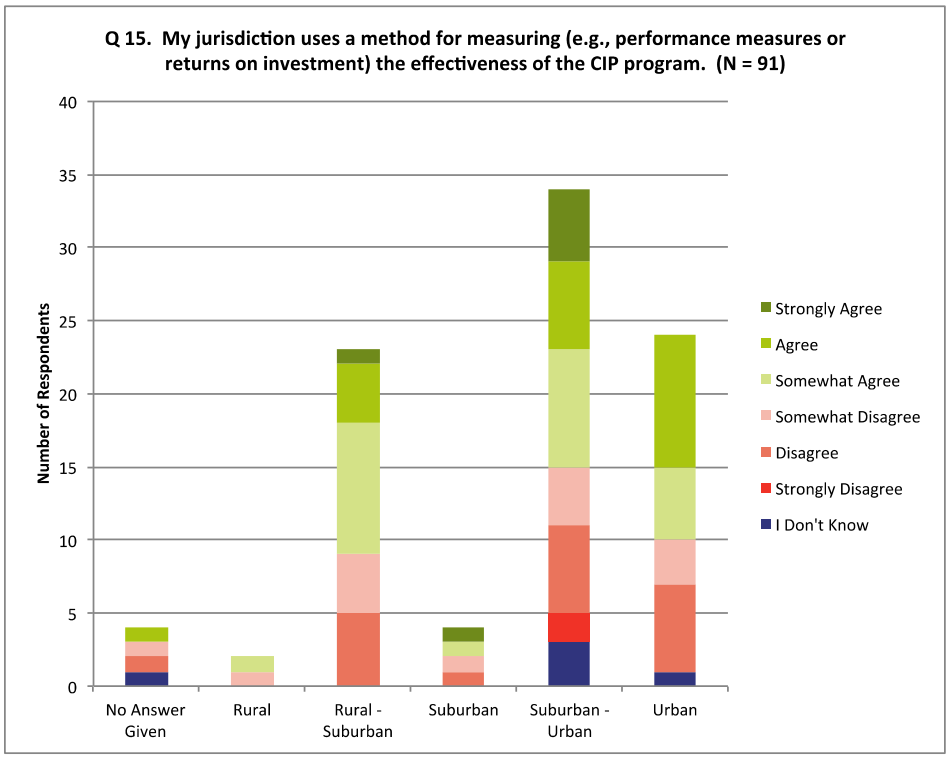


Figure 33A. Figure 33 cross-analyzed by respondents qualified jurisdiction.

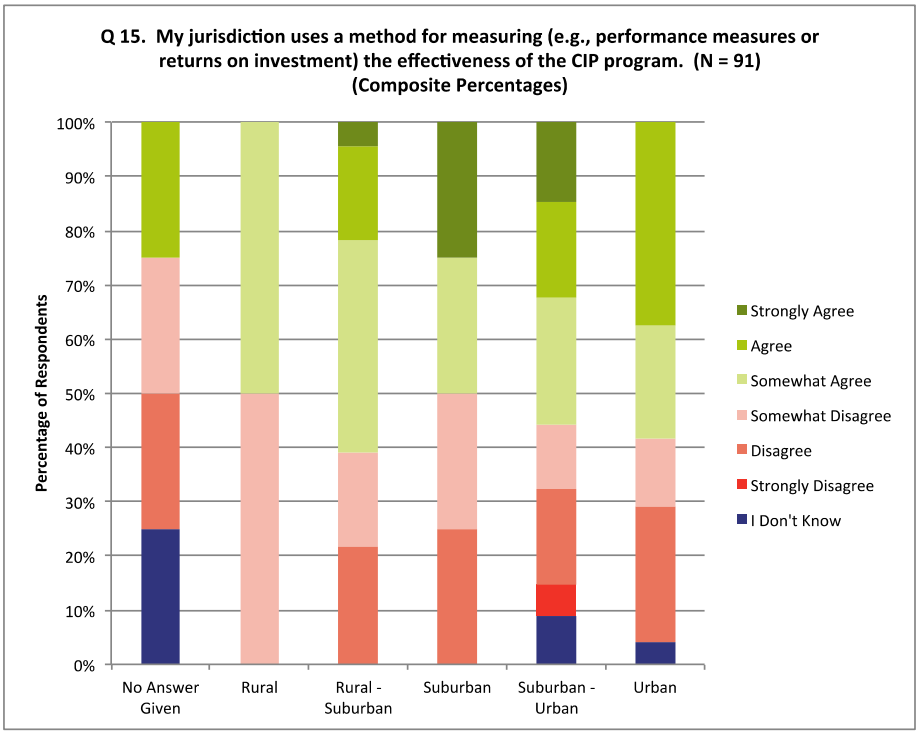


Figure 33B. Composite percentages of Figure 33A.

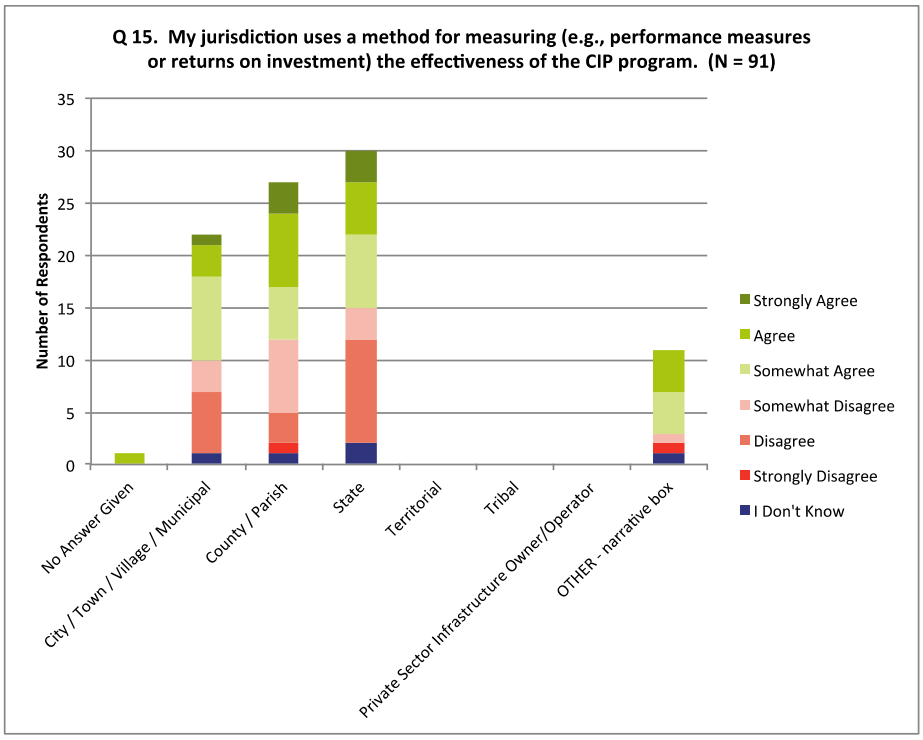


Figure 33C. Figure 33 cross-analyzed by respondents qualified jurisdiction.

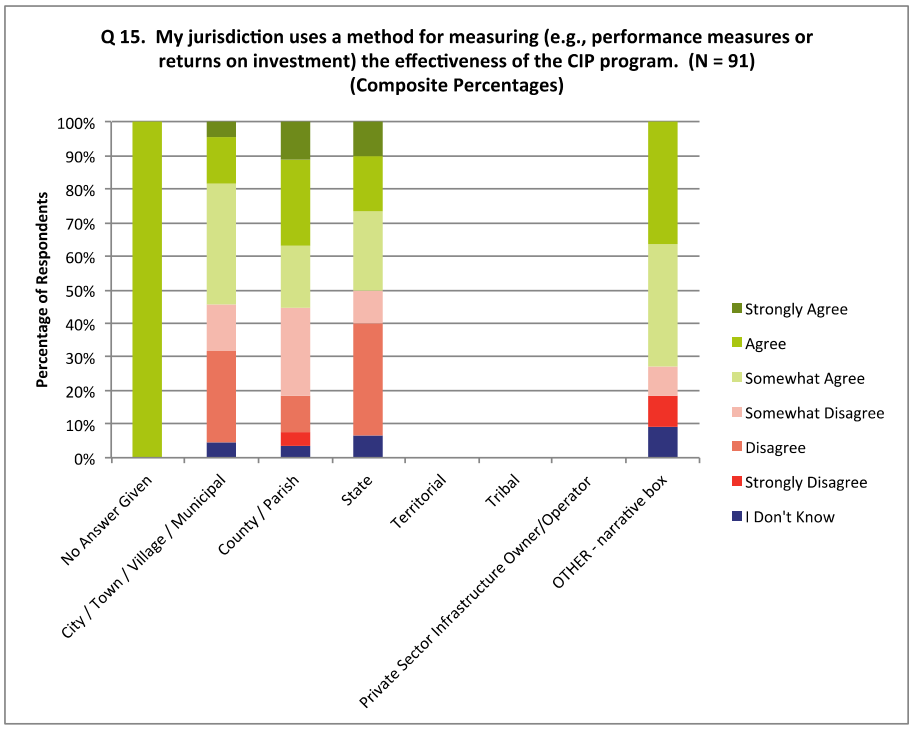


Figure 33D. Composite percentages of Figure 33C.

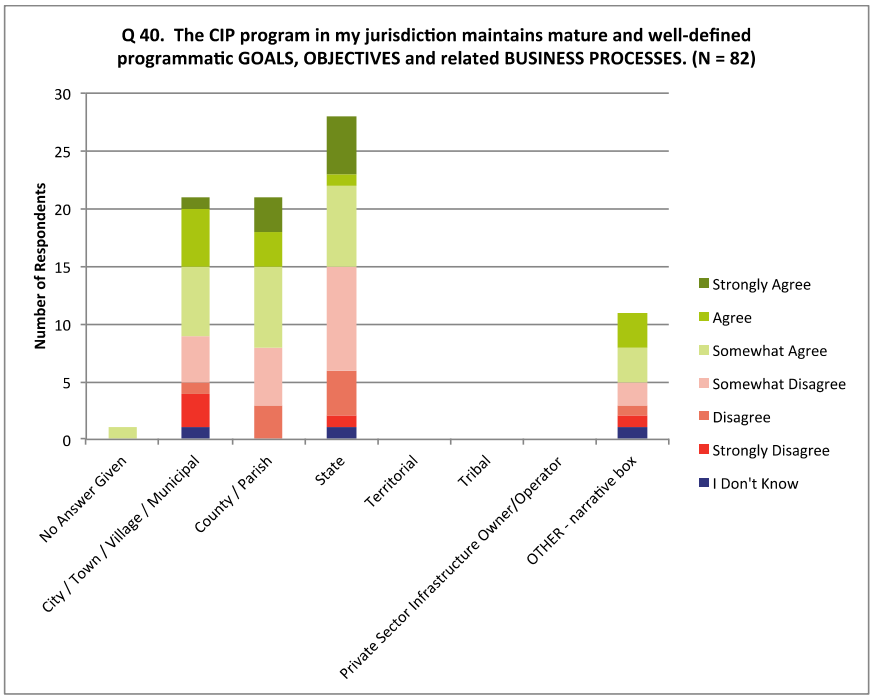


Figure 34C. Figure 34 cross-analyzed by respondents jurisdiction type.

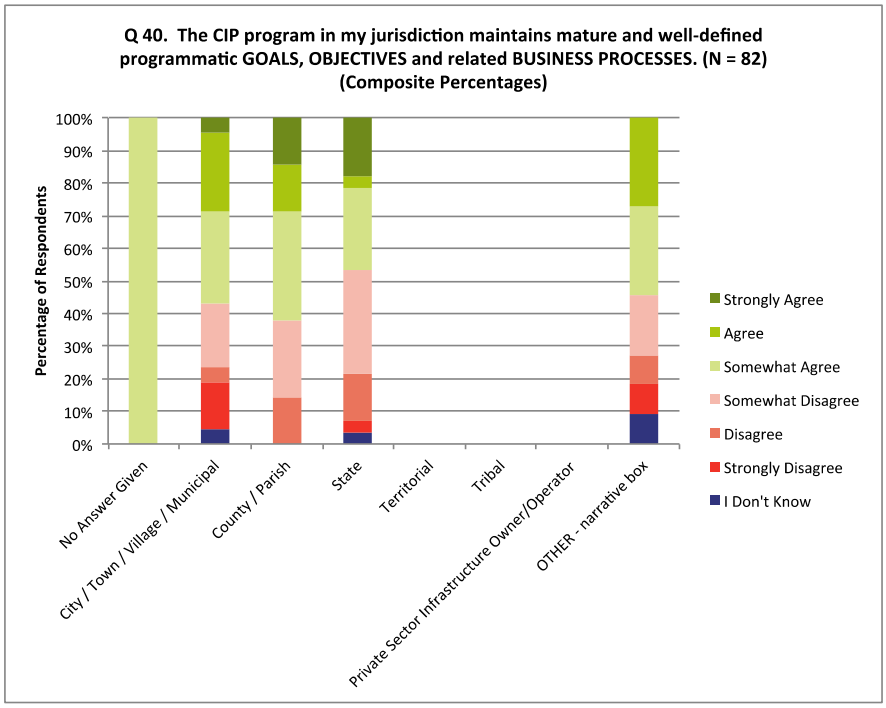


Figure 34D. Composite percentages of Figure 34C.

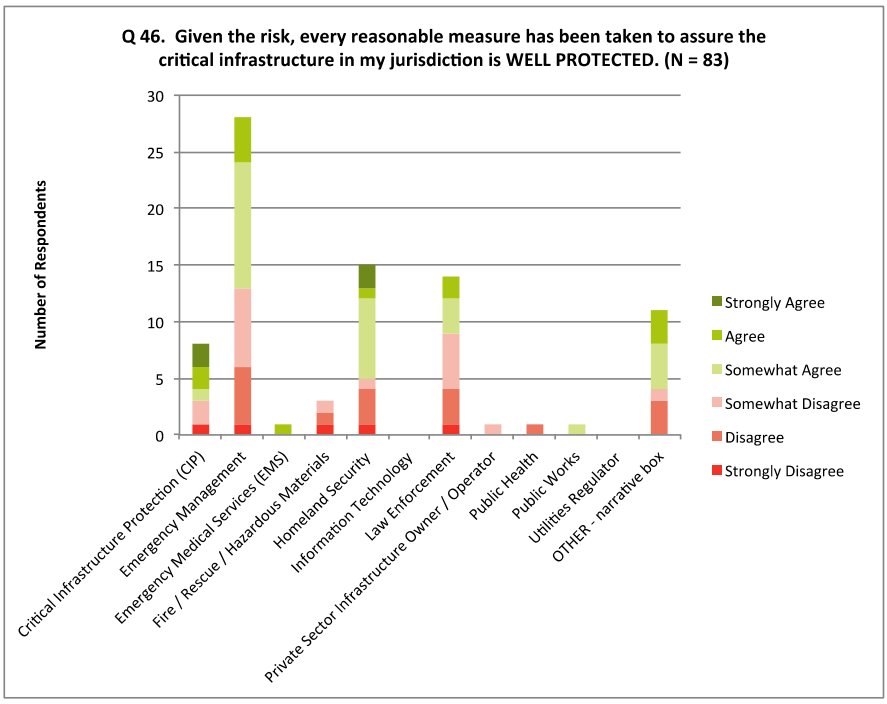


Figure 37A. Figure 37 cross-analyzed by respondents organization type.

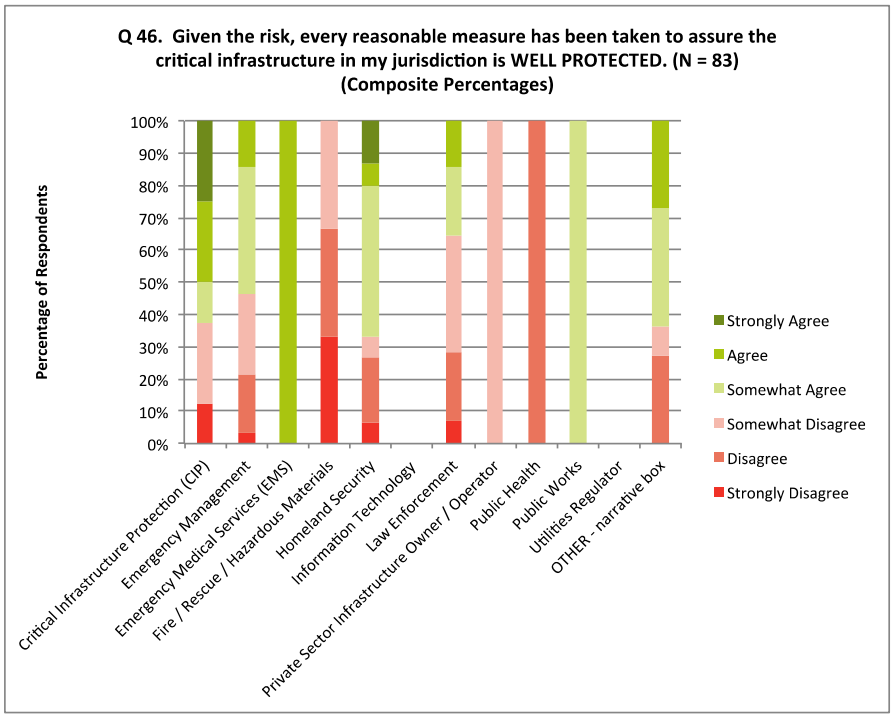


Figure 37B. Composite percentages of Figure 37A.

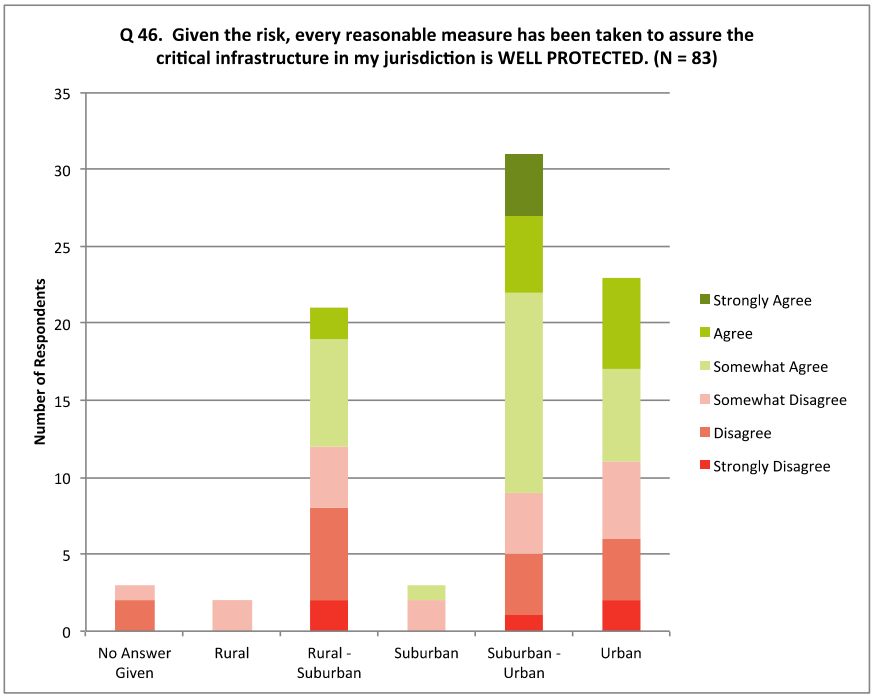


Figure 37C. Figure 37 cross-analyzed by respondents qualified jurisdiction.

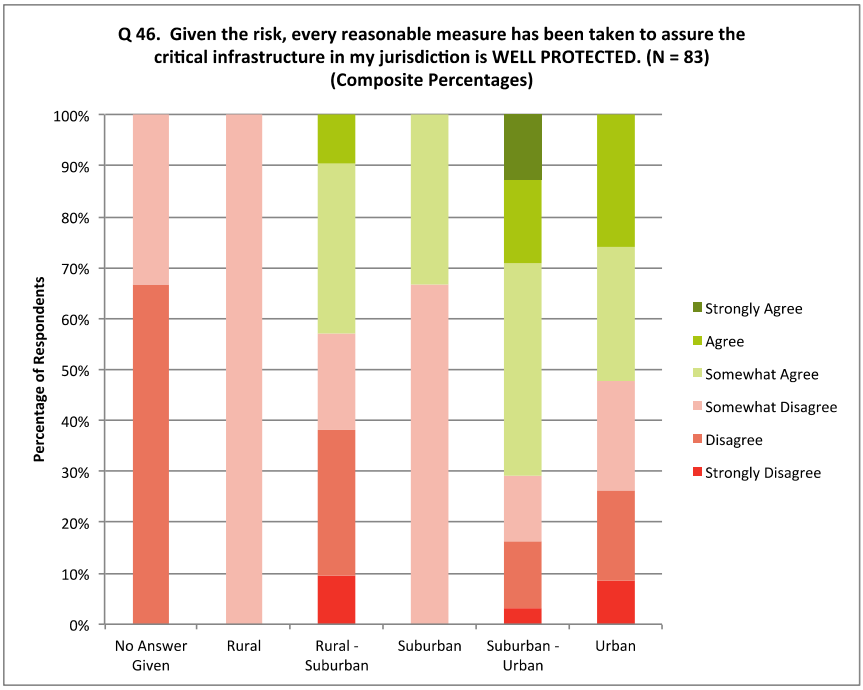


Figure 37D. Composite percentages of Figure 37C.

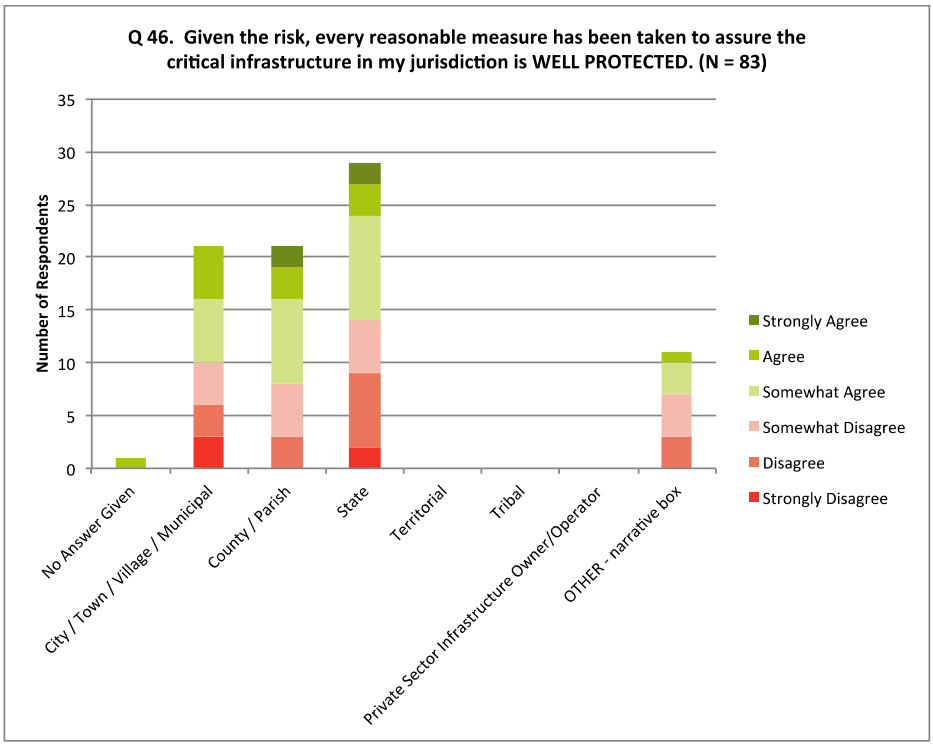


Figure 37E. Figure 37 cross-analyzed by respondents jurisdiction type.

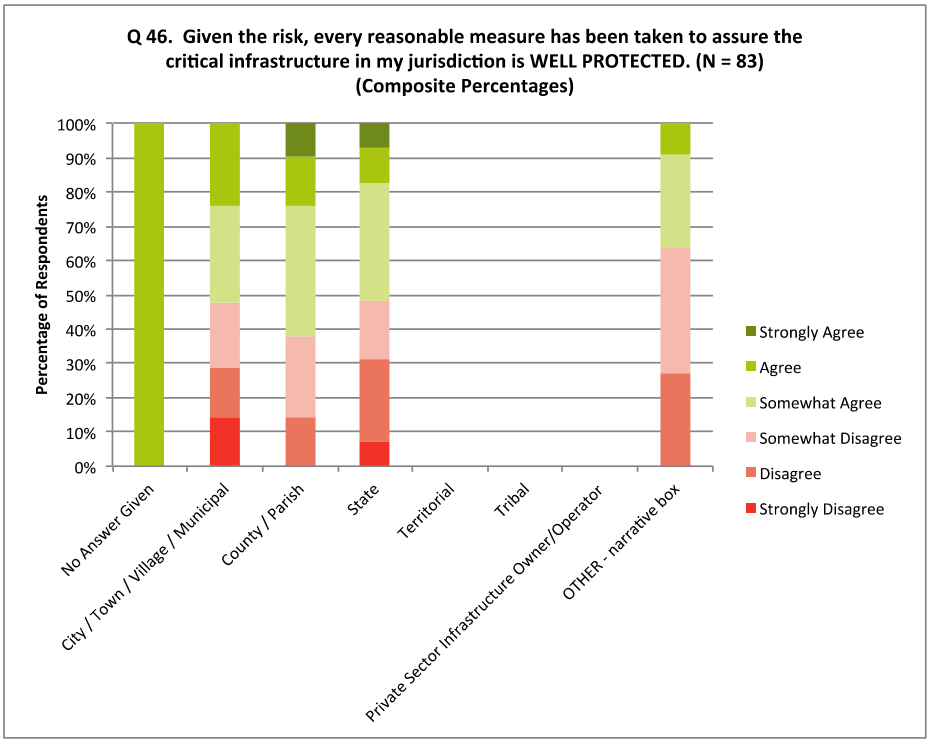


Figure 37F. Composite percentages of Figure 37E.

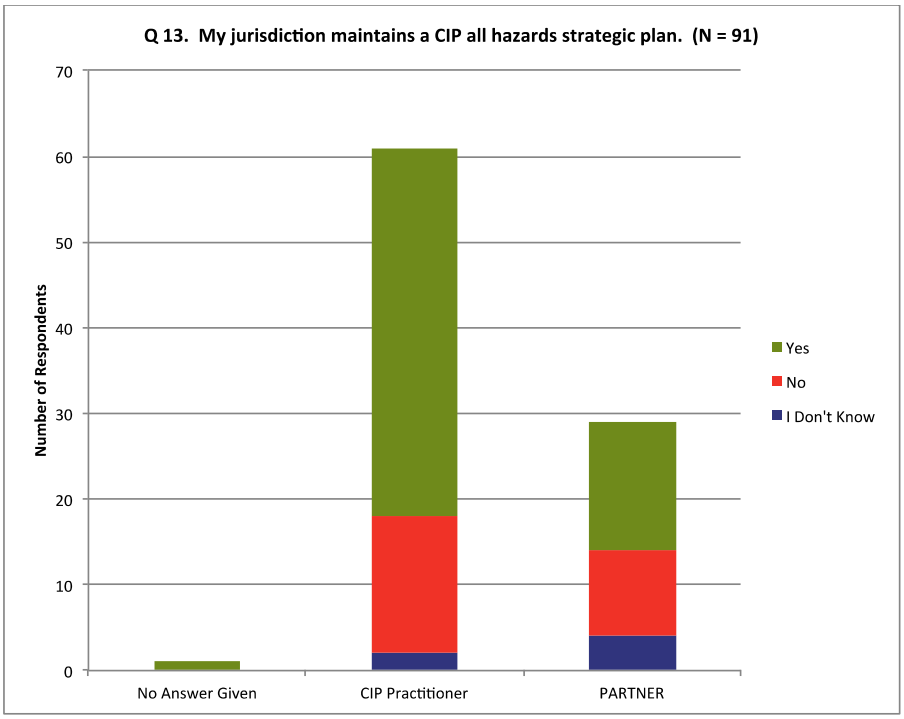


Figure 38A. Figure 38 cross-analyzed by respondents that self-identify as a CIP practitioner or partner.

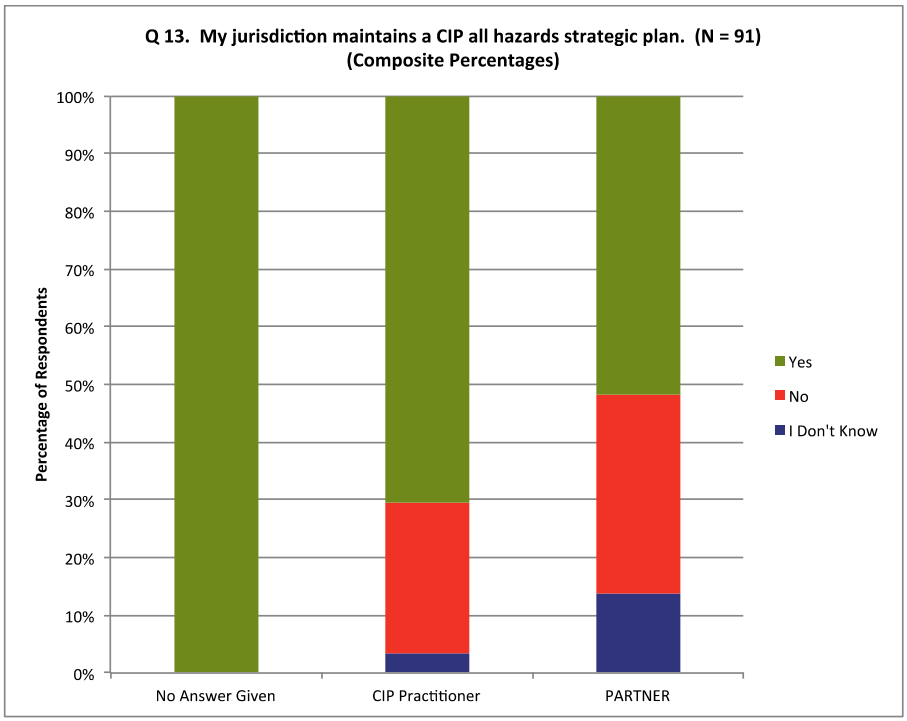


Figure 38B. Composite percentages of Figure 38A.

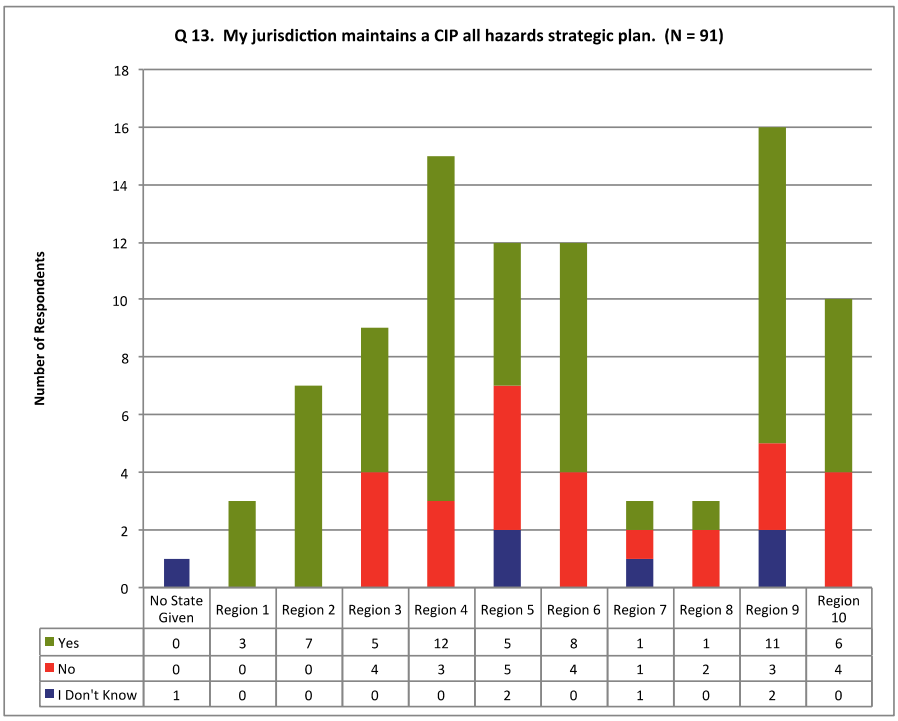


Figure 38C. Figure 38 cross-analyzed by respondents federal FEMA region.

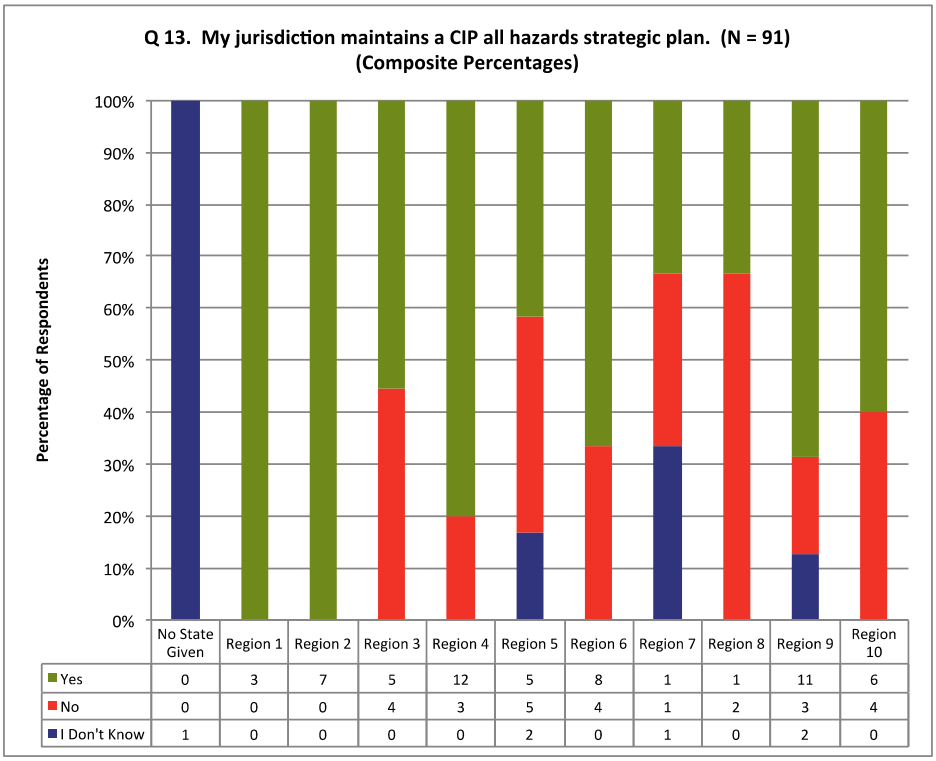


Figure 38D. Composite percentages of Figure 38C.

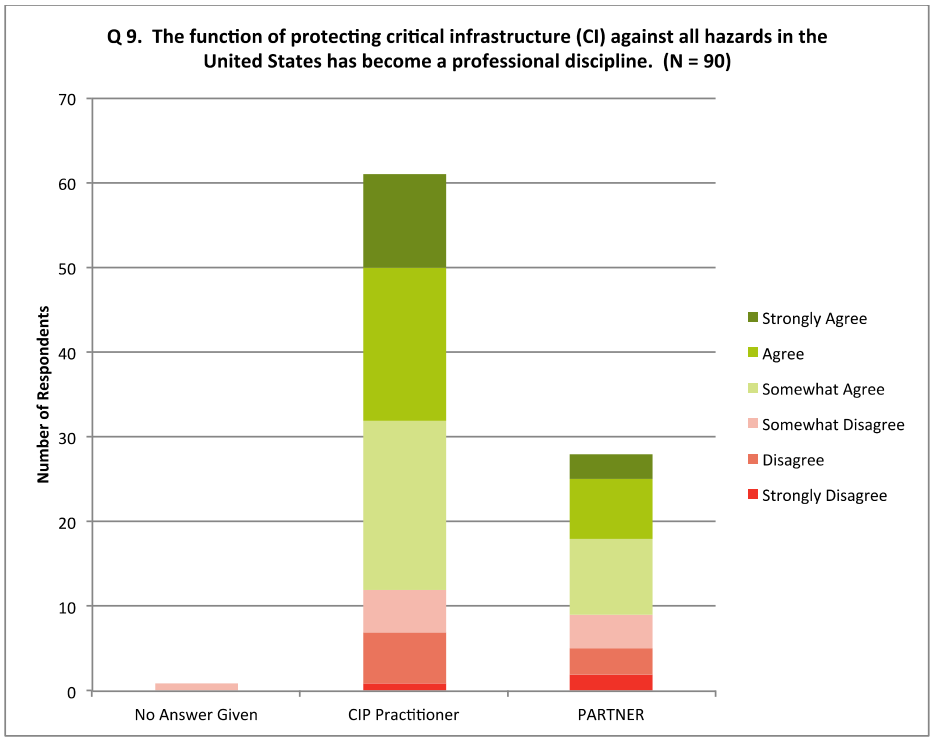


Figure 39A. Figure 39 cross-analyzed by respondents that self-identify as a CIP practitioner or partner.

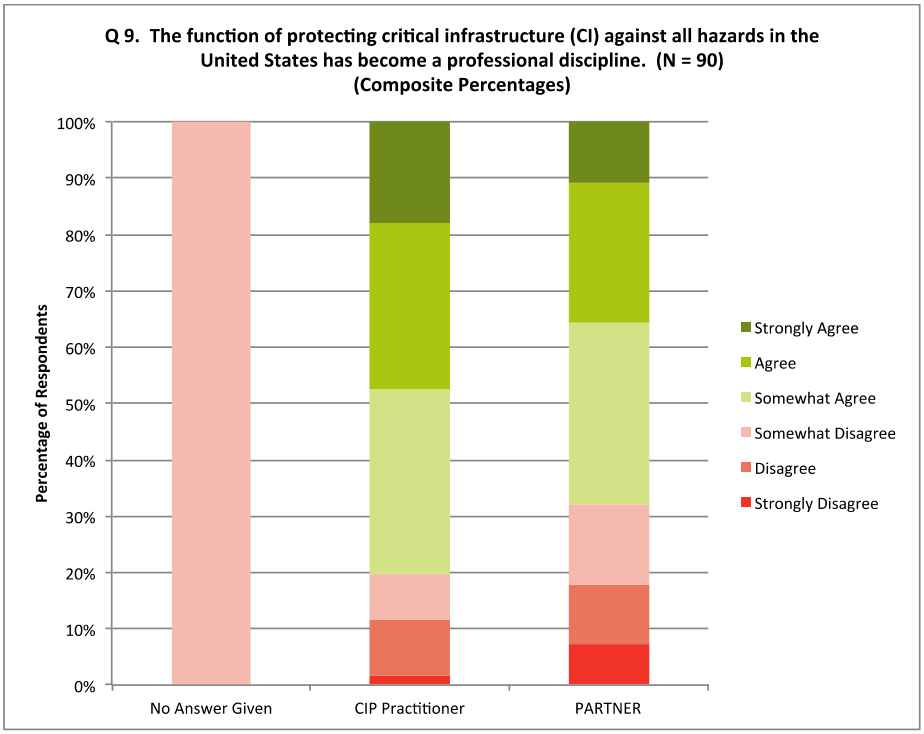


Figure 39B. Composite percentages of Figure 39A.

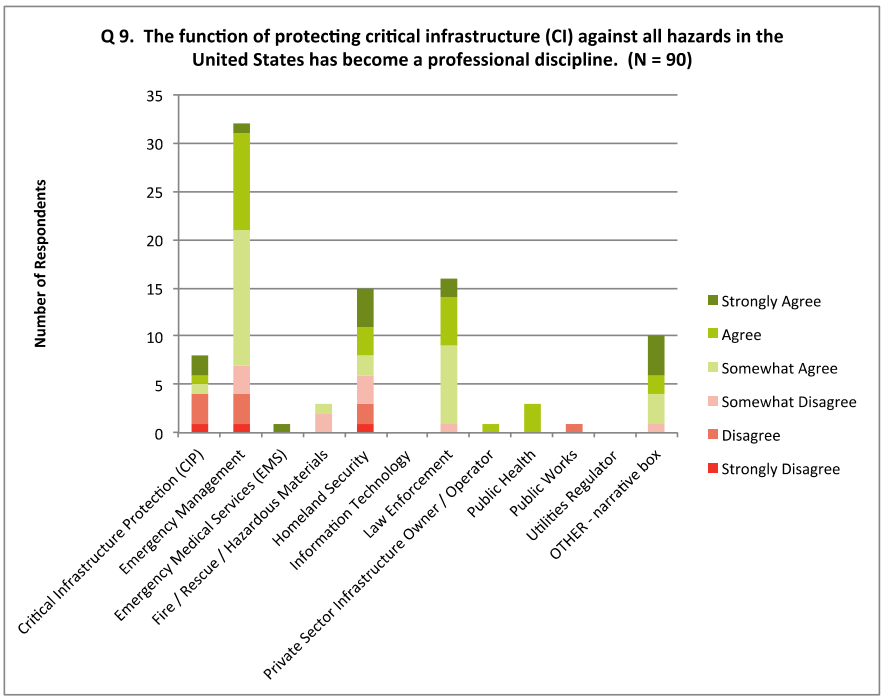


Figure 39C. Figure 39 cross-analyzed by respondents organization type.

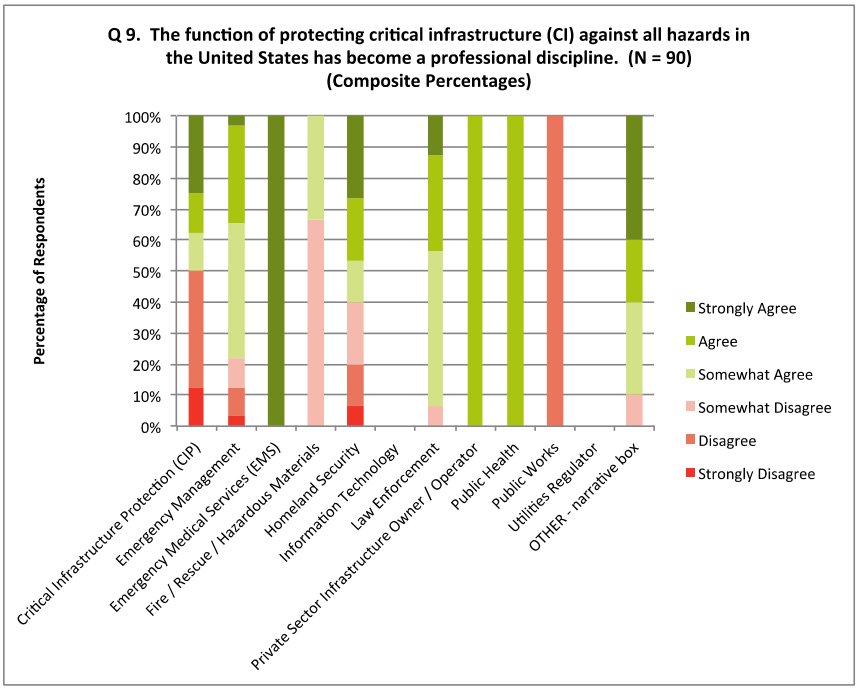


Figure 39D. Composite percentages of Figure 39C.

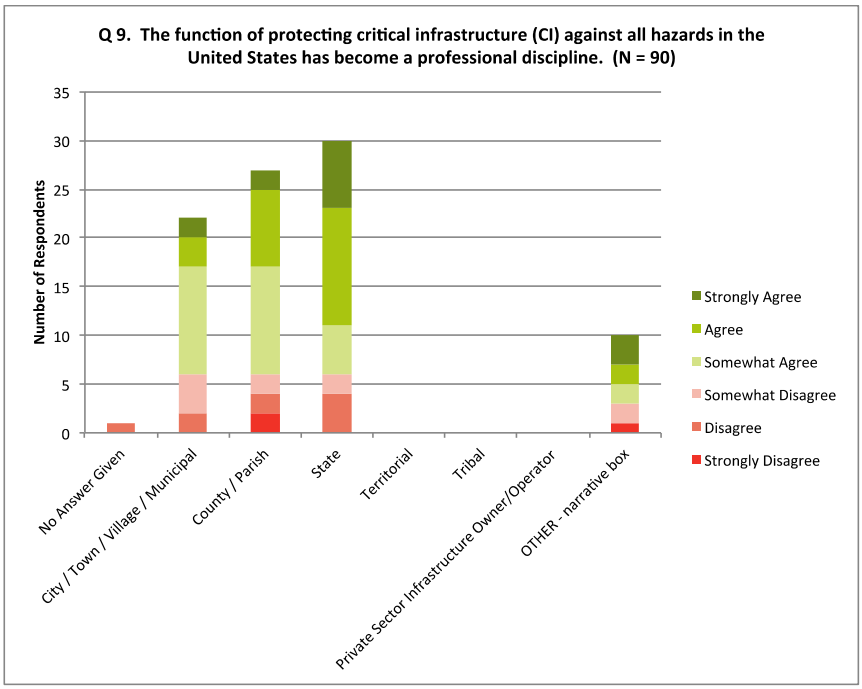


Figure 39E. Figure 39 cross-analyzed by respondents jurisdiction type.

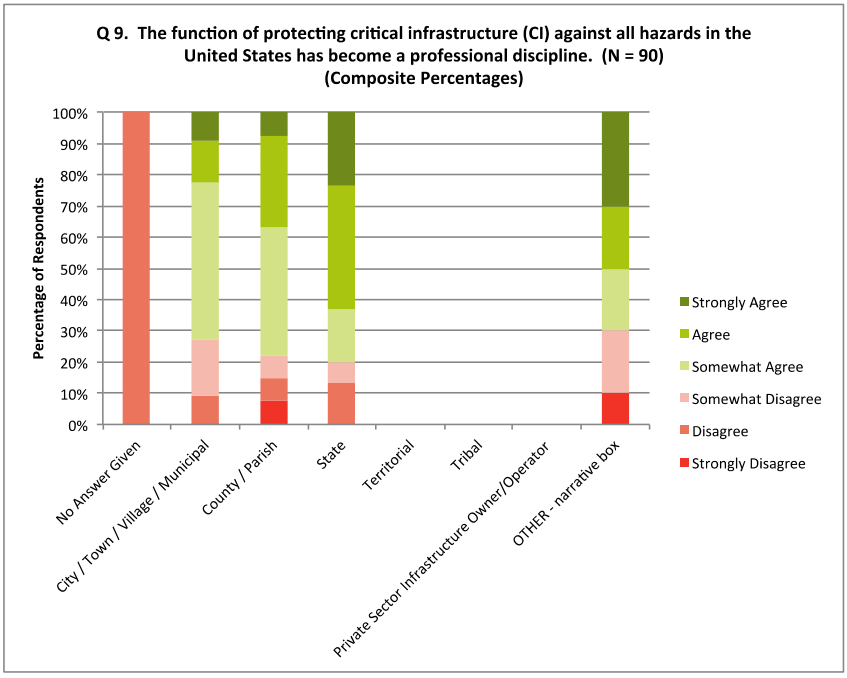
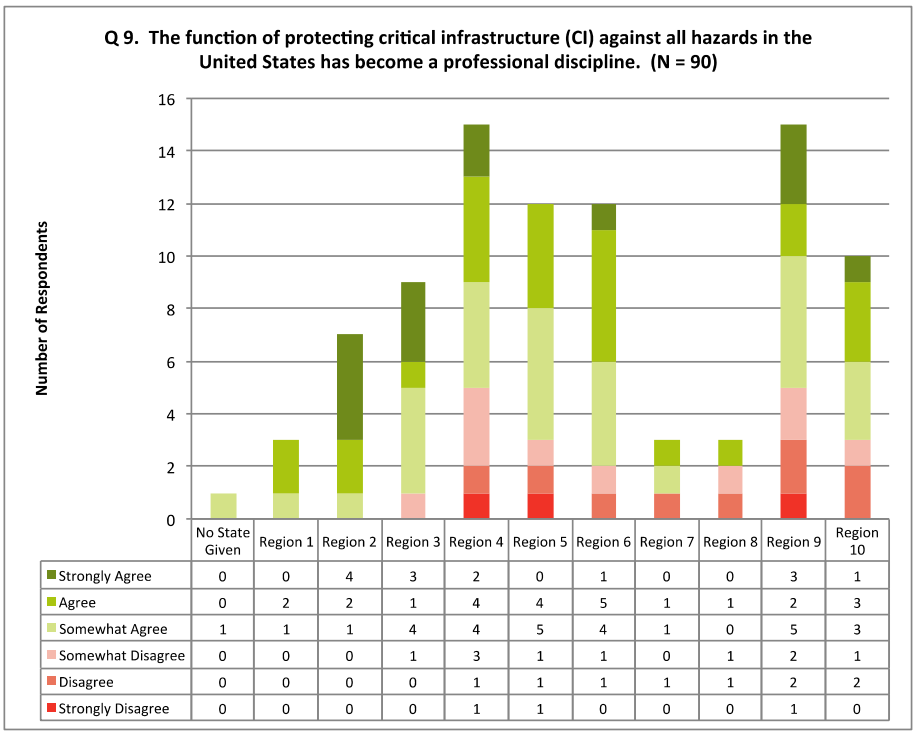
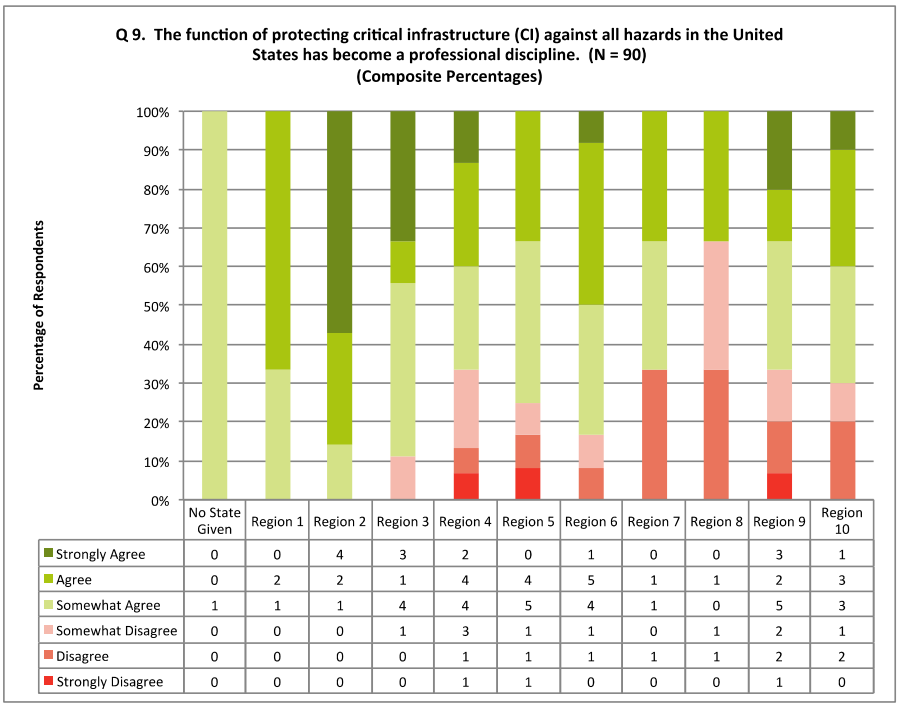


Figure 39F. Composite percentages of Figure 39E.



	No State Given	Region 1	Region 2	Region 3	Region 4	Region 5	Region 6	Region 7	Region 8	Region 9	Region 10
Strongly Agree	0	0	4	3	2	0	1	0	0	3	1
Agree	0	2	2	1	4	4	5	1	1	2	3
Somewhat Agree	1	1	1	4	4	5	4	1	0	5	3
Somewhat Disagree	0	0	0	1	3	1	1	0	1	2	1
Disagree	0	0	0	0	1	1	1	1	1	2	2
Strongly Disagree	0	0	0	0	1	1	0	0	0	1	0

Figure 39G. Figure 39 cross-analyzed by respondents federal FEMA region.



	No State Given	Region 1	Region 2	Region 3	Region 4	Region 5	Region 6	Region 7	Region 8	Region 9	Region 10
Strongly Agree	0	0	4	3	2	0	1	0	0	3	1
Agree	0	2	2	1	4	4	5	1	1	2	3
Somewhat Agree	1	1	1	4	4	5	4	1	0	5	3
Somewhat Disagree	0	0	0	1	3	1	1	0	1	2	1
Disagree	0	0	0	0	1	1	1	1	1	2	2
Strongly Disagree	0	0	0	0	1	1	0	0	0	1	0

Figure 39H. Composite percentages of Figure 39G.

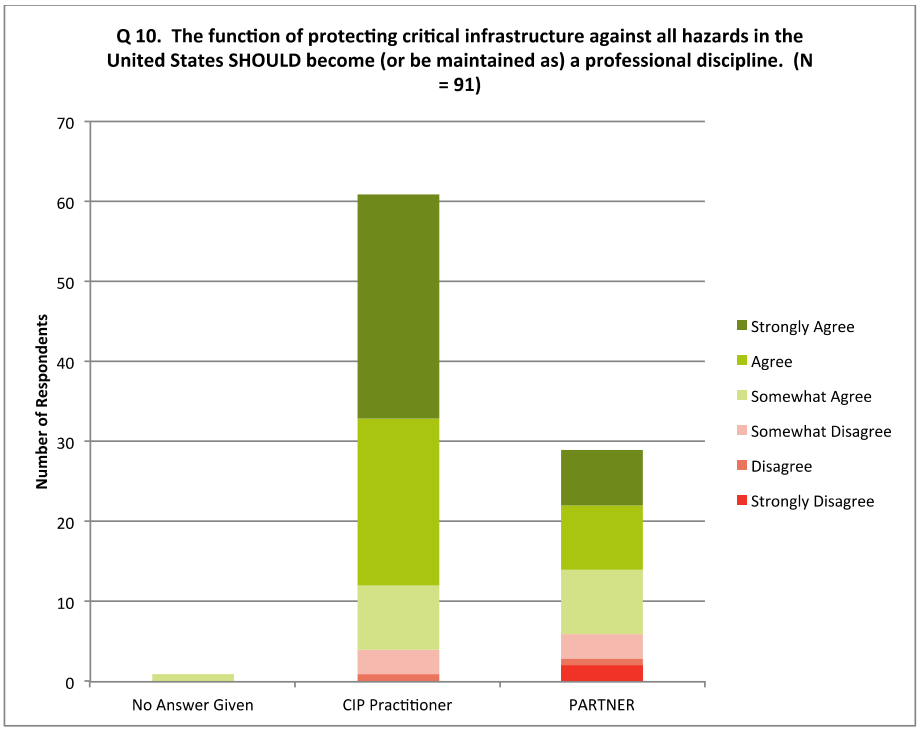


Figure 40A. Figure 40 cross-analyzed by respondents that self-identify as a CIP practitioner or partner.

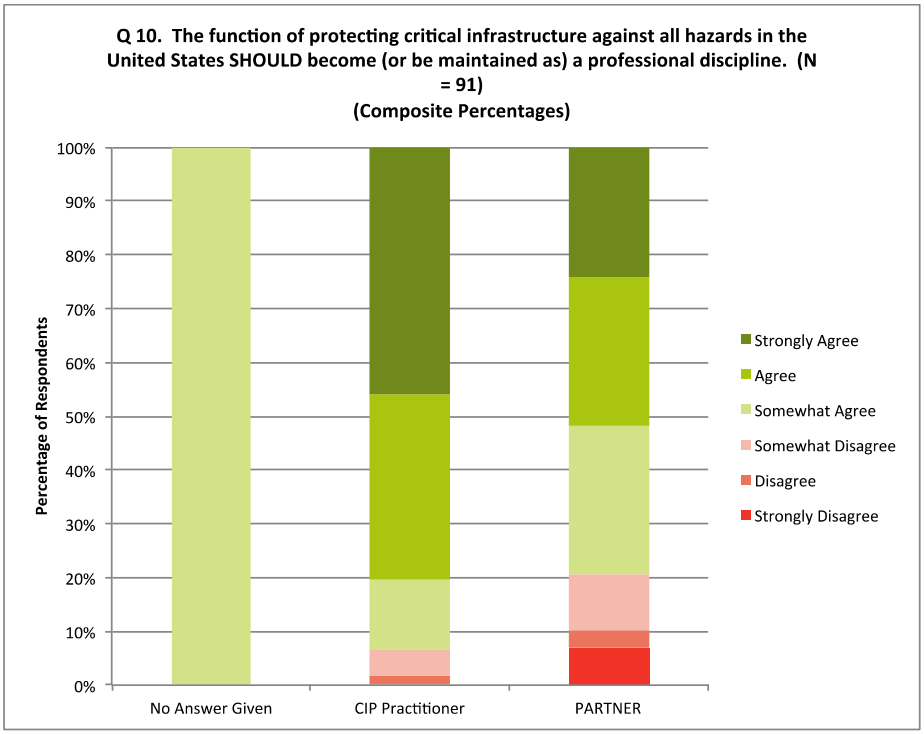


Figure 40B. Composite percentages of Figure 40A.

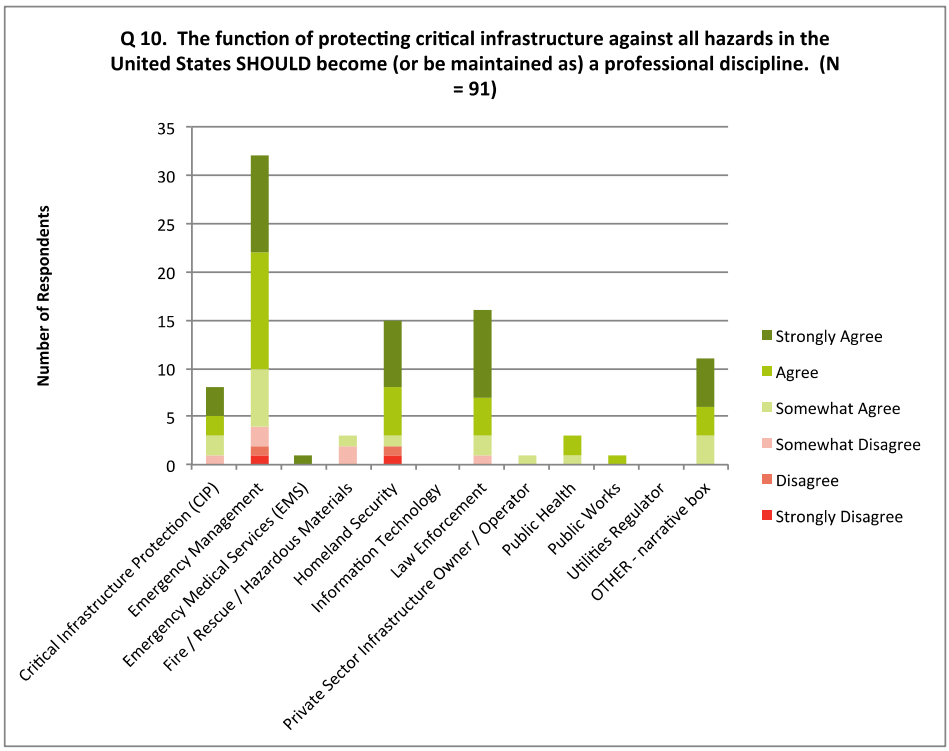


Figure 40C. Figure 40 cross-analyzed by respondents organization type.

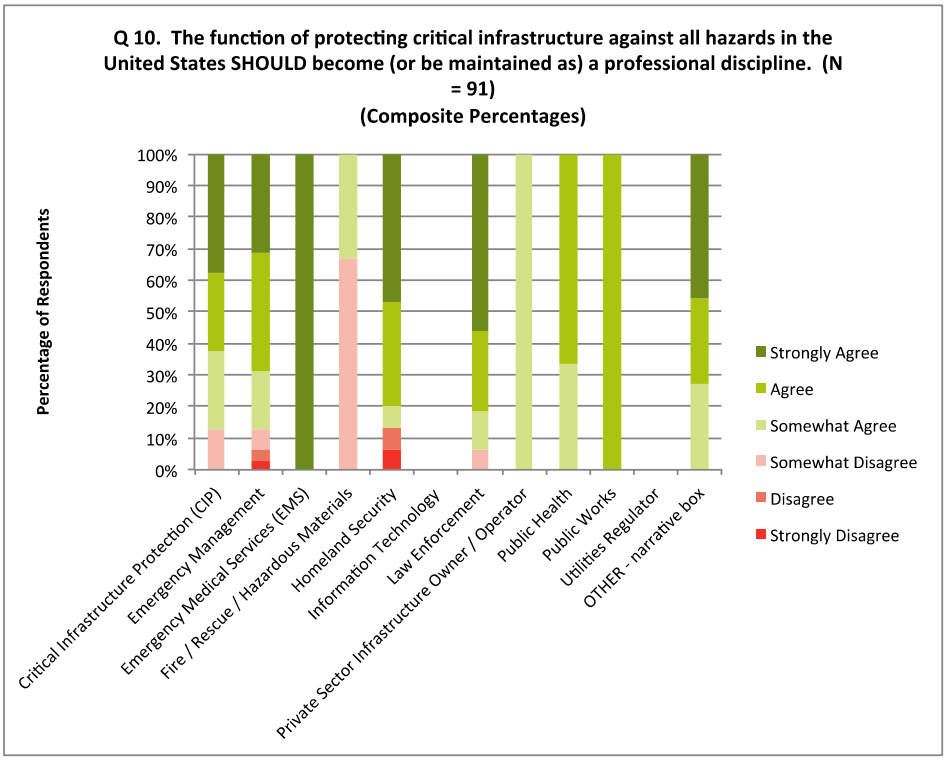


Figure 40D. Composite percentages of Figure 40C.

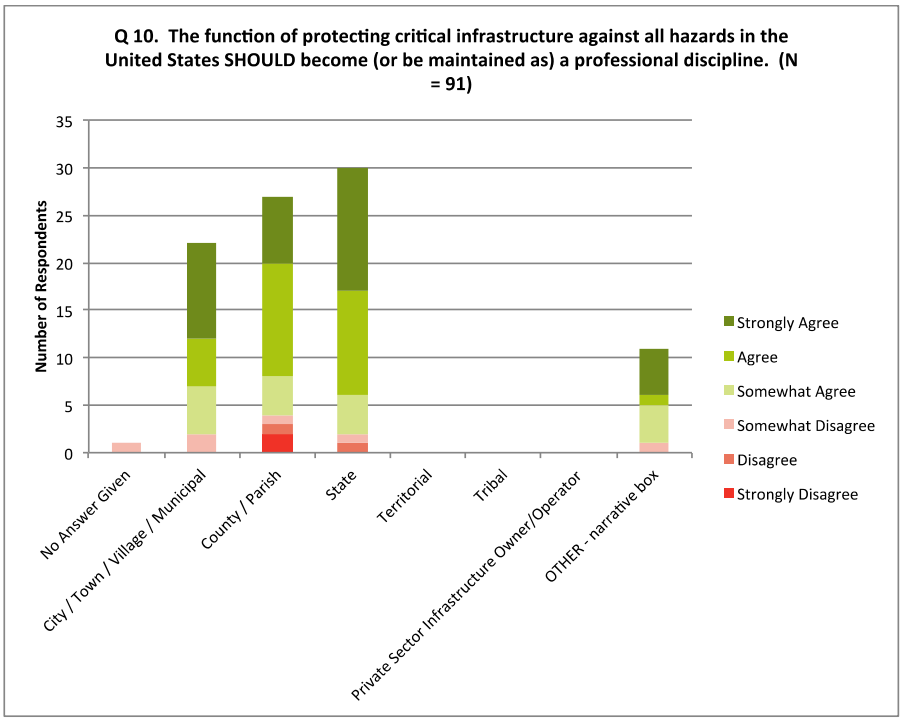


Figure 340E. Figure 40 cross-analyzed by respondents jurisdiction type.

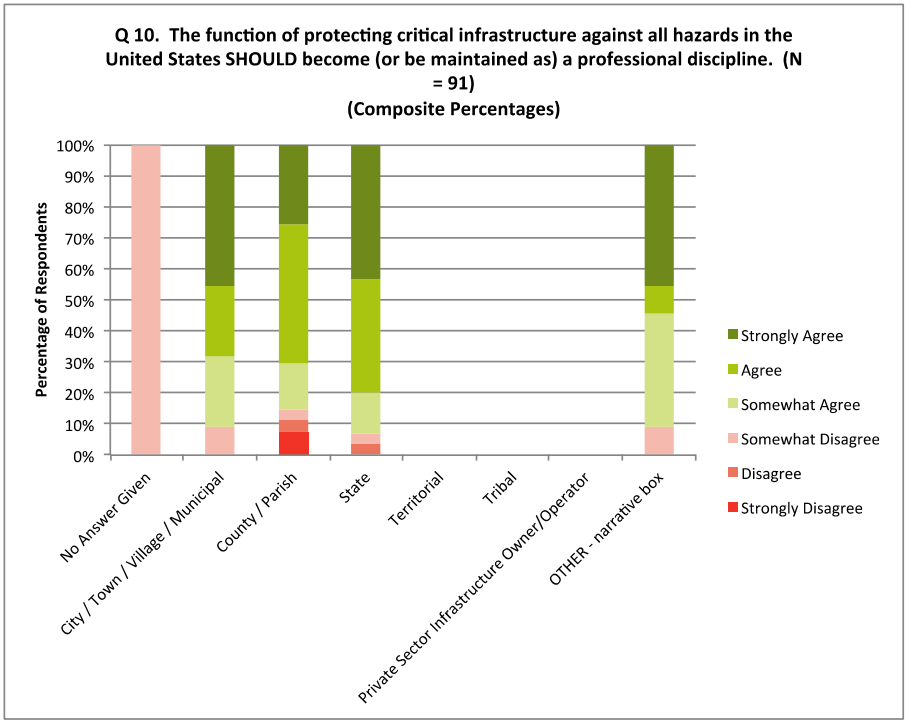
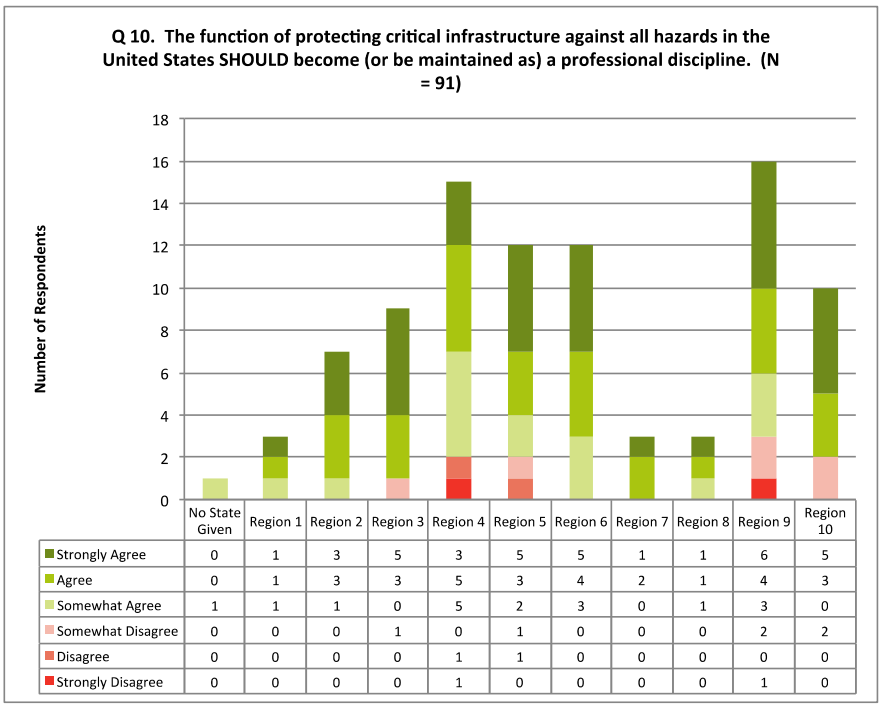
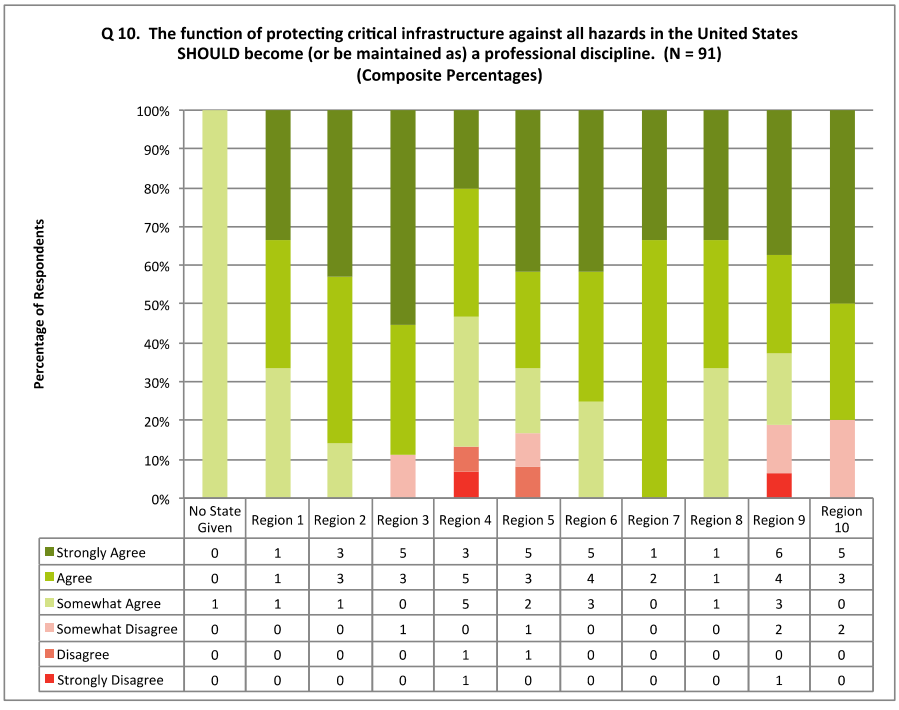


Figure 40F. Composite percentages of Figure 40E.



	No State Given	Region 1	Region 2	Region 3	Region 4	Region 5	Region 6	Region 7	Region 8	Region 9	Region 10
Strongly Agree	0	1	3	5	3	5	5	1	1	6	5
Agree	0	1	3	3	5	3	4	2	1	4	3
Somewhat Agree	1	1	1	0	5	2	3	0	1	3	0
Somewhat Disagree	0	0	0	1	0	1	0	0	0	2	2
Disagree	0	0	0	0	1	1	0	0	0	0	0
Strongly Disagree	0	0	0	0	1	0	0	0	0	1	0

Figure 40G. Figure 40 cross-analyzed by respondents federal FEMA region.



	No State Given	Region 1	Region 2	Region 3	Region 4	Region 5	Region 6	Region 7	Region 8	Region 9	Region 10
Strongly Agree	0	1	3	5	3	5	5	1	1	6	5
Agree	0	1	3	3	5	3	4	2	1	4	3
Somewhat Agree	1	1	1	0	5	2	3	0	1	3	0
Somewhat Disagree	0	0	0	1	0	1	0	0	0	2	2
Disagree	0	0	0	0	1	1	0	0	0	0	0
Strongly Disagree	0	0	0	0	1	0	0	0	0	1	0

Figure 40H. Composite percentages of Figure 40G.

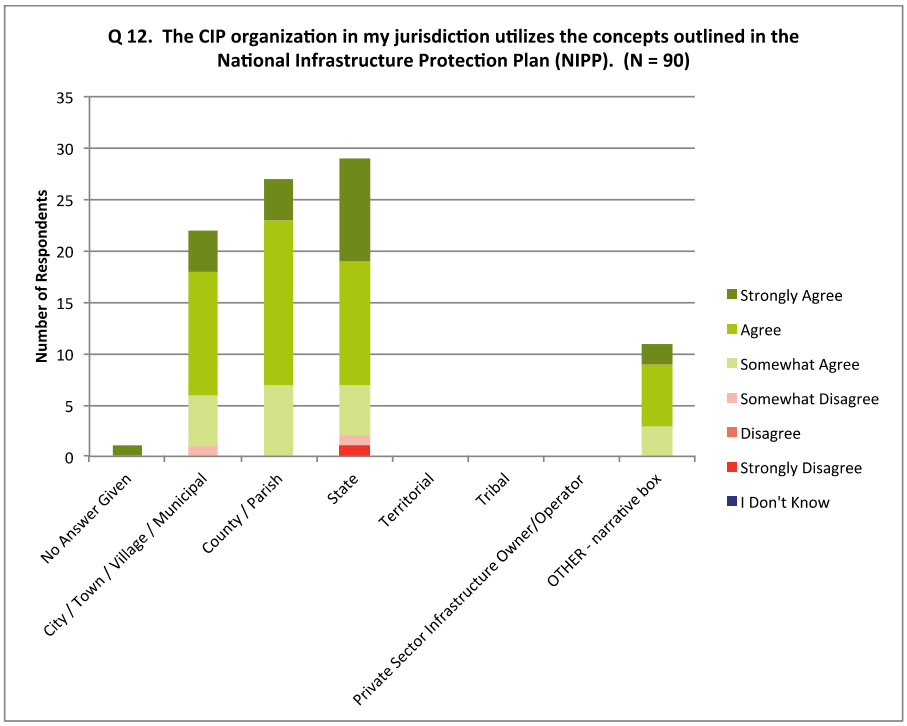


Figure 41A. Figure 41 cross-analyzed by respondents jurisdiction type.

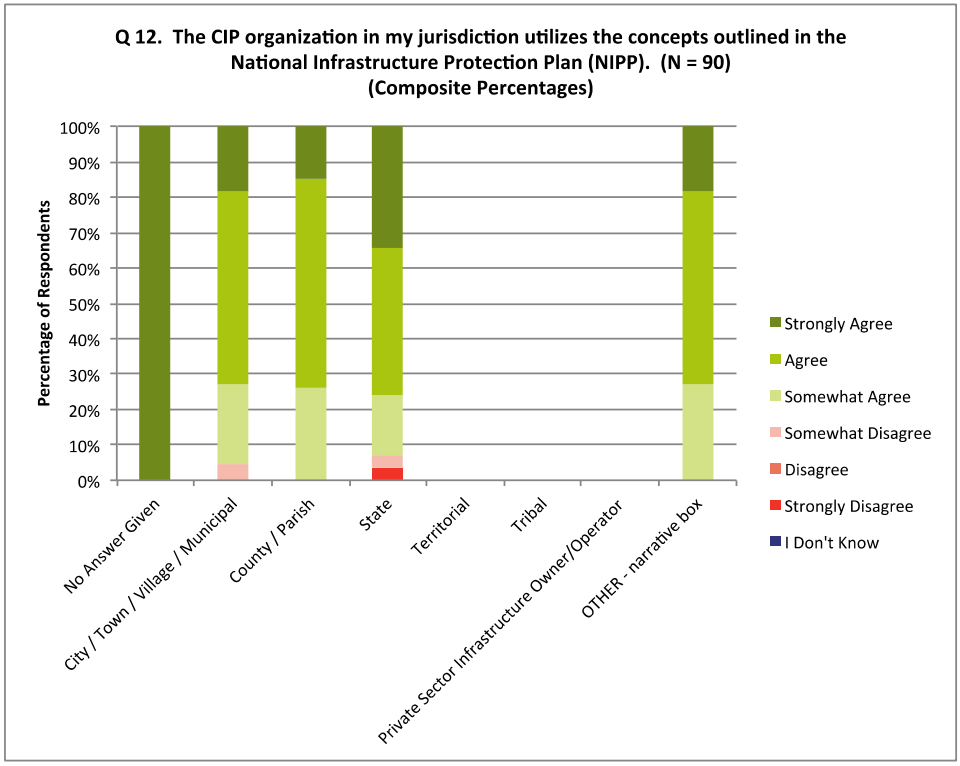
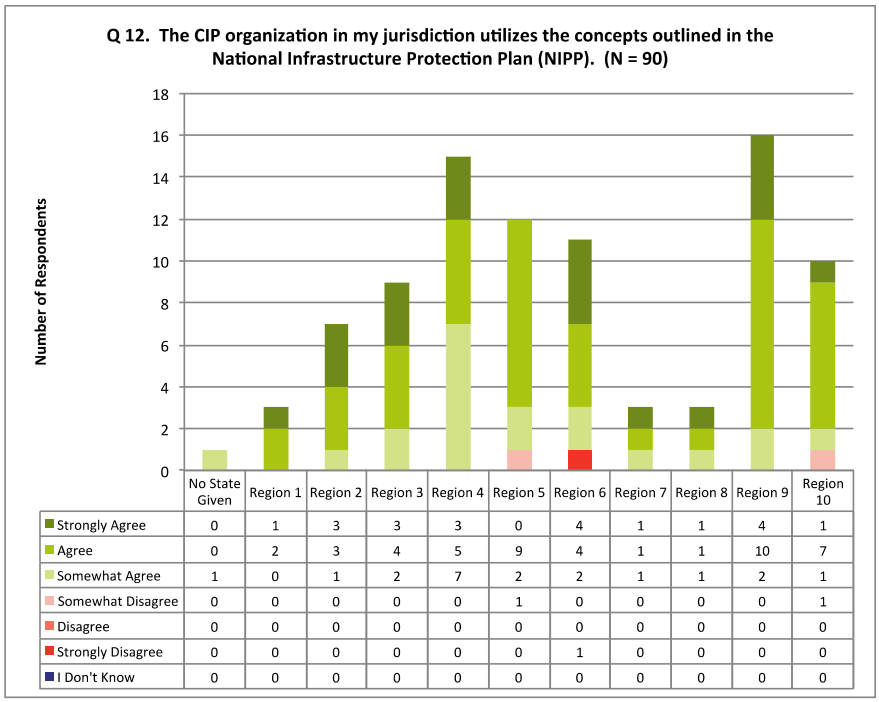
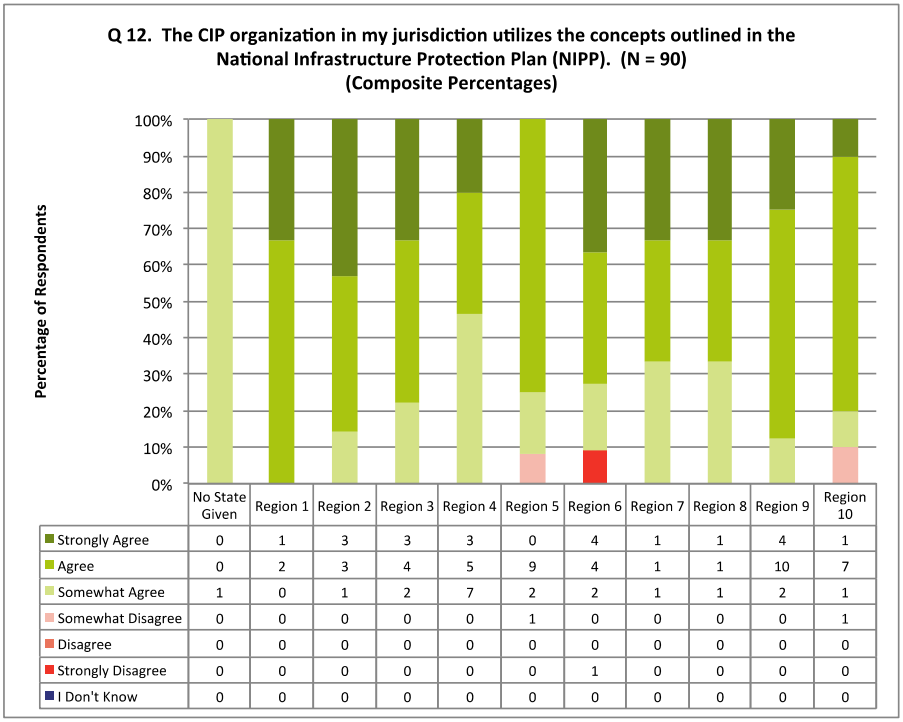


Figure 41B. Composite percentages of Figure 41A.



	No State Given	Region 1	Region 2	Region 3	Region 4	Region 5	Region 6	Region 7	Region 8	Region 9	Region 10
Strongly Agree	0	1	3	3	3	0	4	1	1	4	1
Agree	0	2	3	4	5	9	4	1	1	10	7
Somewhat Agree	1	0	1	2	7	2	2	1	1	2	1
Somewhat Disagree	0	0	0	0	0	1	0	0	0	0	1
Disagree	0	0	0	0	0	0	0	0	0	0	0
Strongly Disagree	0	0	0	0	0	0	1	0	0	0	0
I Don't Know	0	0	0	0	0	0	0	0	0	0	0

Figure 41C. Figure 41 cross-analyzed by respondents federal FEMA region.



	No State Given	Region 1	Region 2	Region 3	Region 4	Region 5	Region 6	Region 7	Region 8	Region 9	Region 10
Strongly Agree	0	1	3	3	3	0	4	1	1	4	1
Agree	0	2	3	4	5	9	4	1	1	10	7
Somewhat Agree	1	0	1	2	7	2	2	1	1	2	1
Somewhat Disagree	0	0	0	0	0	1	0	0	0	0	1
Disagree	0	0	0	0	0	0	0	0	0	0	0
Strongly Disagree	0	0	0	0	0	0	1	0	0	0	0
I Don't Know	0	0	0	0	0	0	0	0	0	0	0

Figure 41D. Composite percentages of Figure 41C.

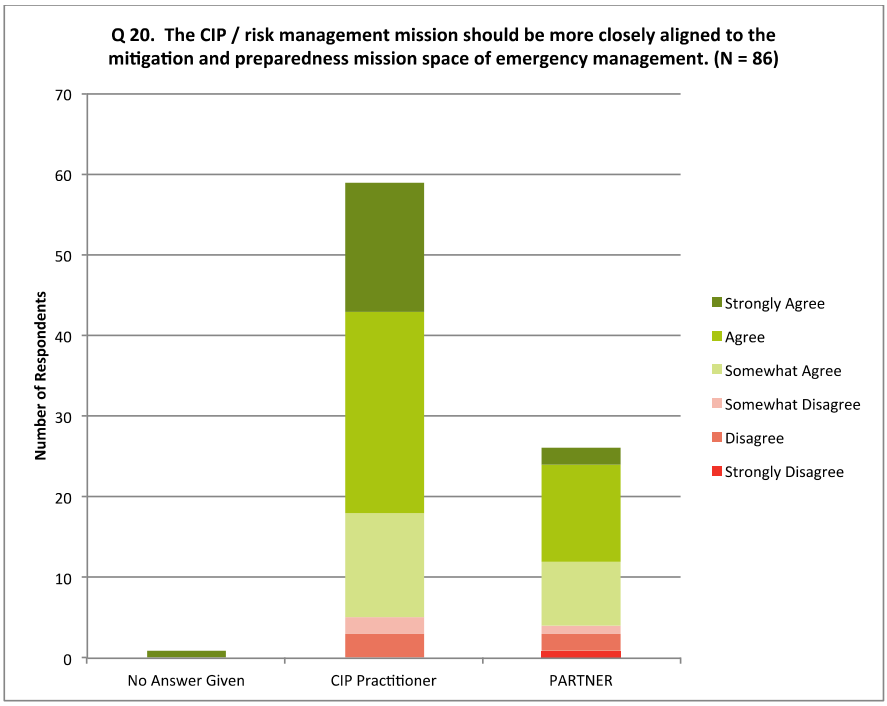


Figure 42A. Figure 42 cross-analyzed by respondents that self-identify as a CIP practitioner or partner.

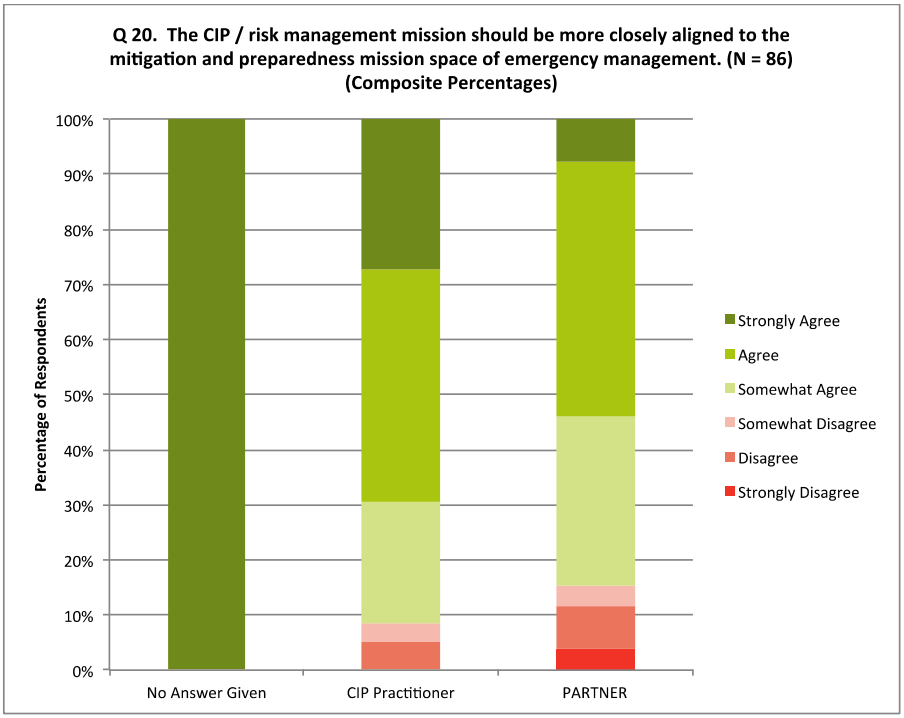


Figure 42B. Composite percentages of Figure 42A.

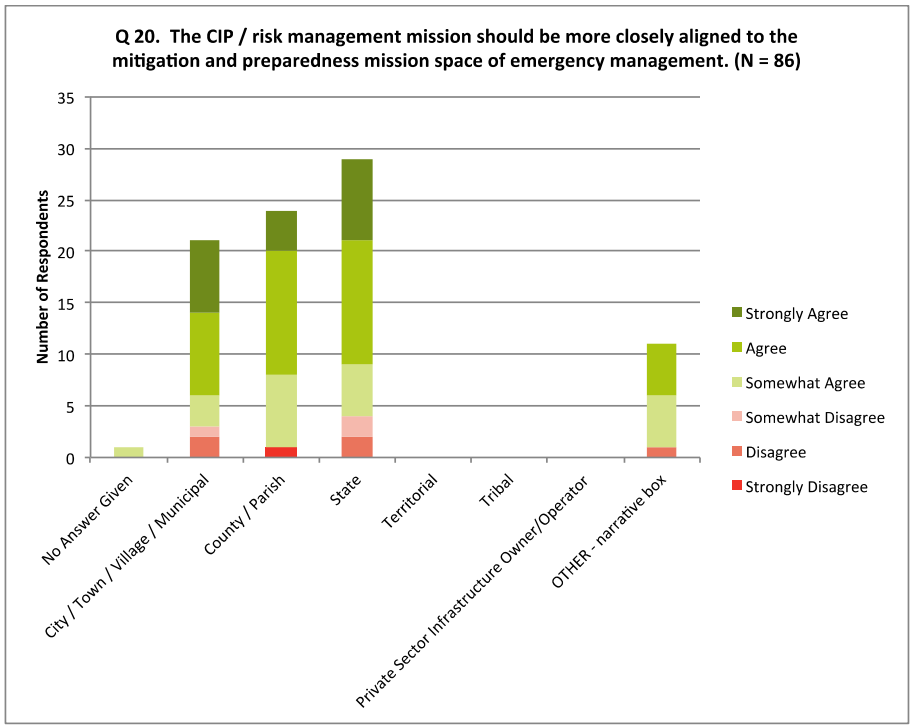


Figure 42E. Figure 42 cross-analyzed by respondents jurisdiction type.

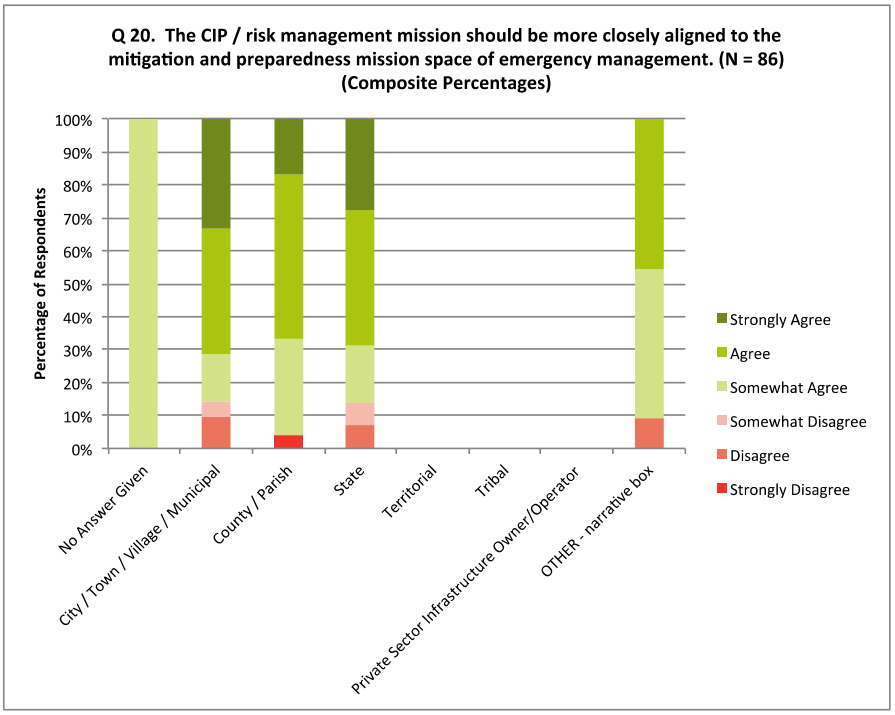


Figure 42F. Composite percentages of Figure 42E.

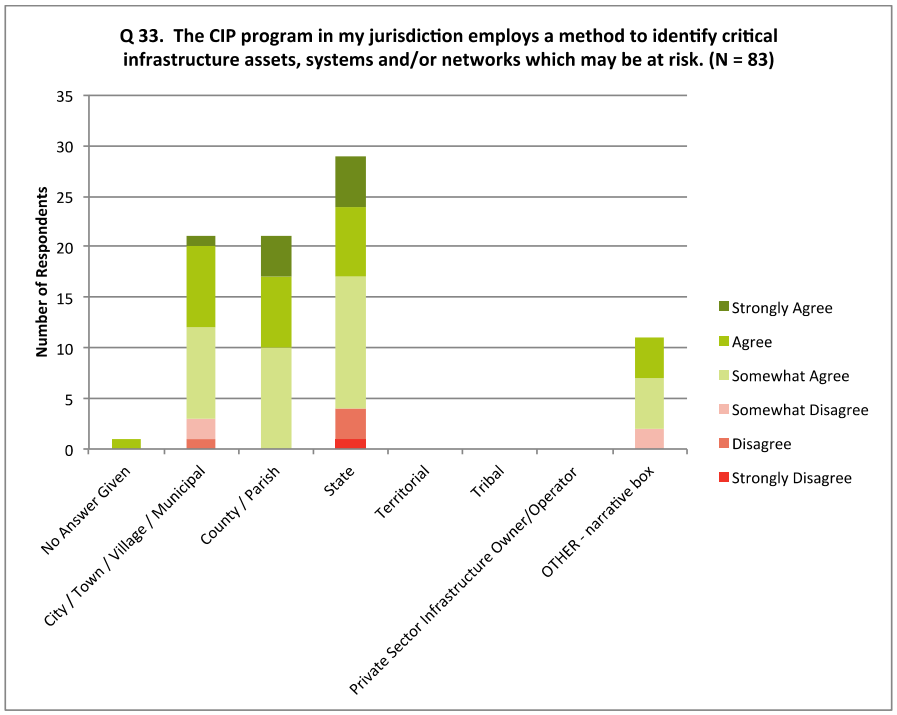


Figure 47A. Figure 47 cross-analyzed by respondents jurisdiction type.

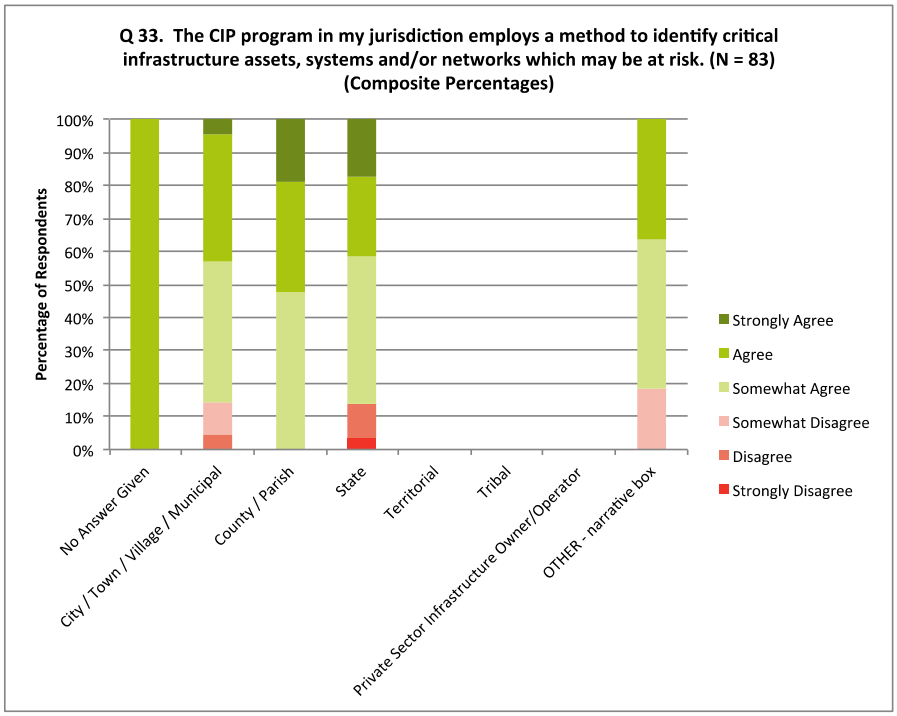
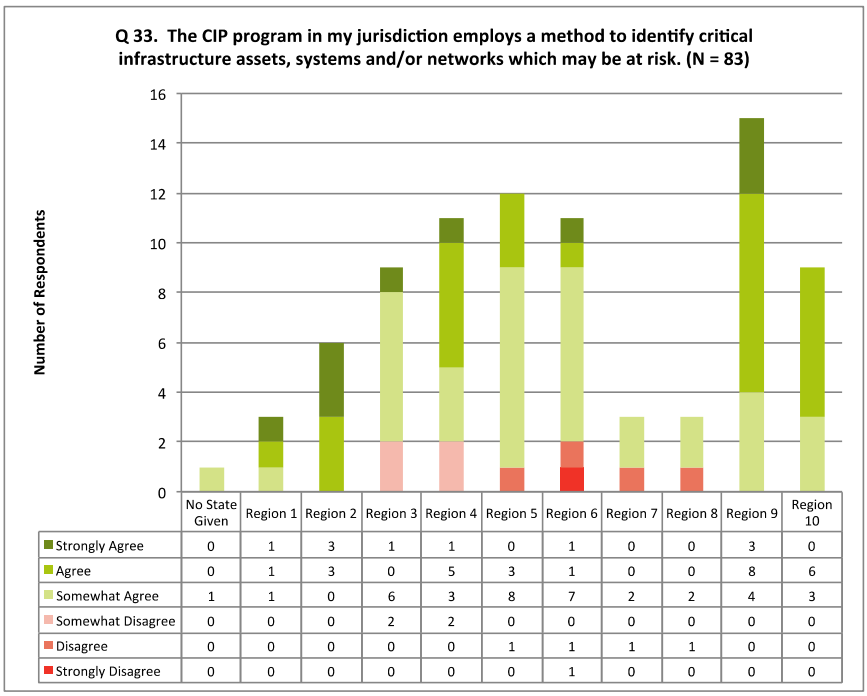
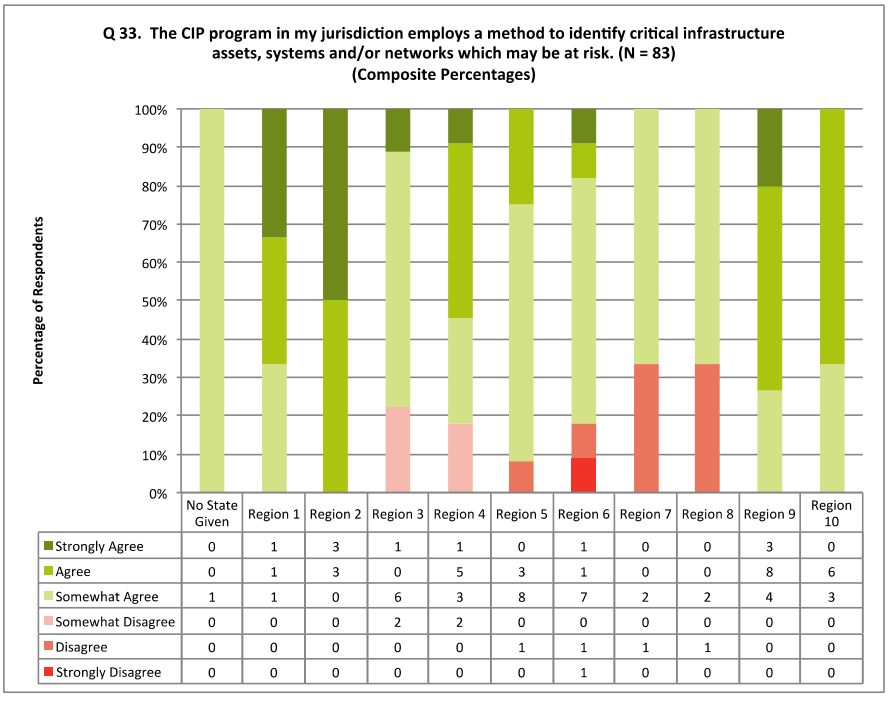


Figure 47B. Composite percentages of Figure 47A.



	No State Given	Region 1	Region 2	Region 3	Region 4	Region 5	Region 6	Region 7	Region 8	Region 9	Region 10
Strongly Agree	0	1	3	1	1	0	1	0	0	3	0
Agree	0	1	3	0	5	3	1	0	0	8	6
Somewhat Agree	1	1	0	6	3	8	7	2	2	4	3
Somewhat Disagree	0	0	0	2	2	0	0	0	0	0	0
Disagree	0	0	0	0	0	1	1	1	1	0	0
Strongly Disagree	0	0	0	0	0	0	1	0	0	0	0

Figure 47C. Figure 47 cross-analyzed by respondents federal FEMA region.



	No State Given	Region 1	Region 2	Region 3	Region 4	Region 5	Region 6	Region 7	Region 8	Region 9	Region 10
Strongly Agree	0	1	3	1	1	0	1	0	0	3	0
Agree	0	1	3	0	5	3	1	0	0	8	6
Somewhat Agree	1	1	0	6	3	8	7	2	2	4	3
Somewhat Disagree	0	0	0	2	2	0	0	0	0	0	0
Disagree	0	0	0	0	0	1	1	1	1	0	0
Strongly Disagree	0	0	0	0	0	0	1	0	0	0	0

Figure 47D. Composite percentages of Figure 47C.

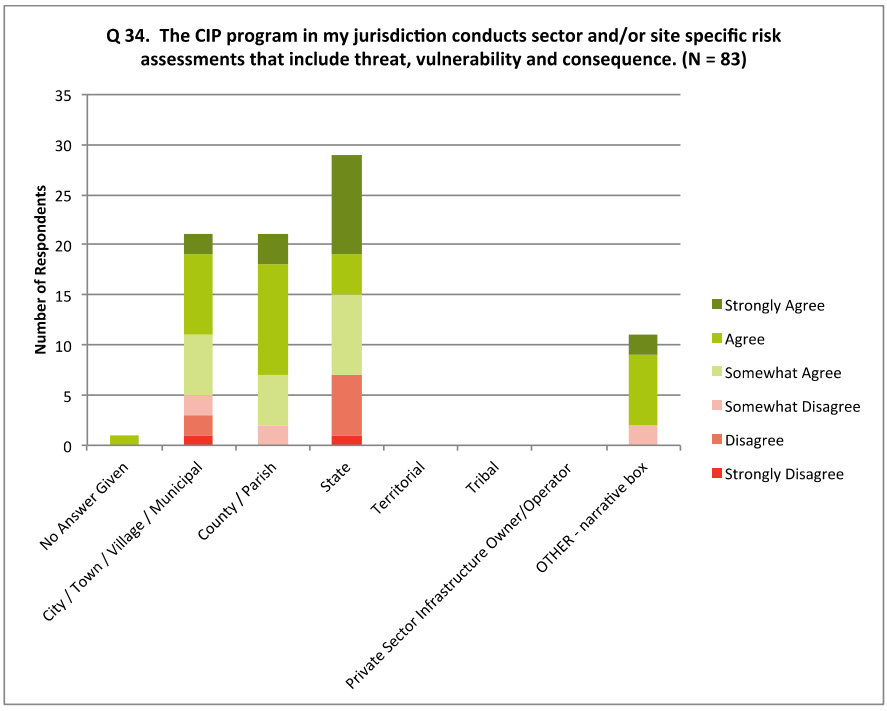


Figure 48A. Figure 48 cross-analyzed by respondents jurisdiction type.

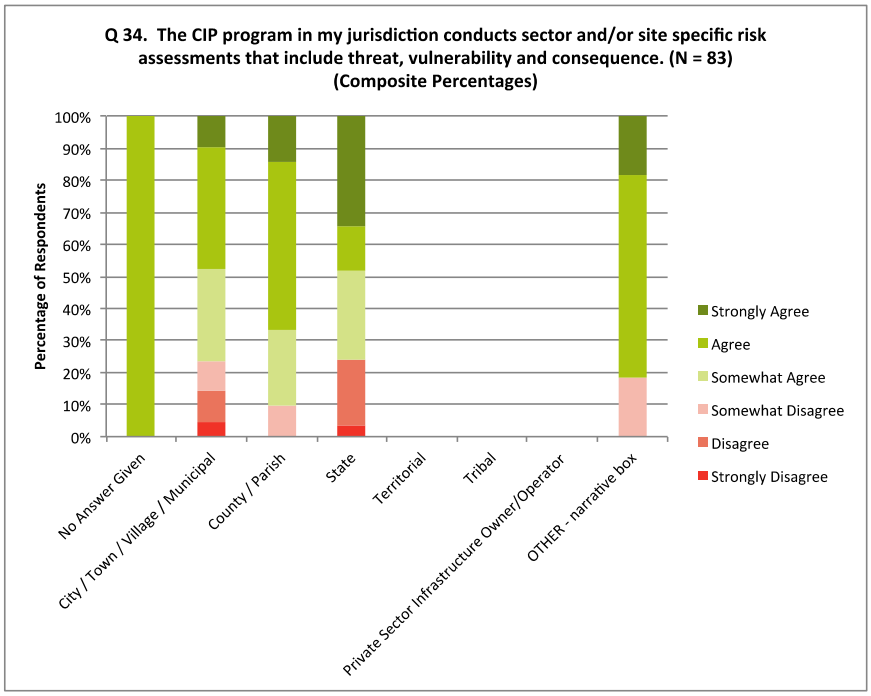
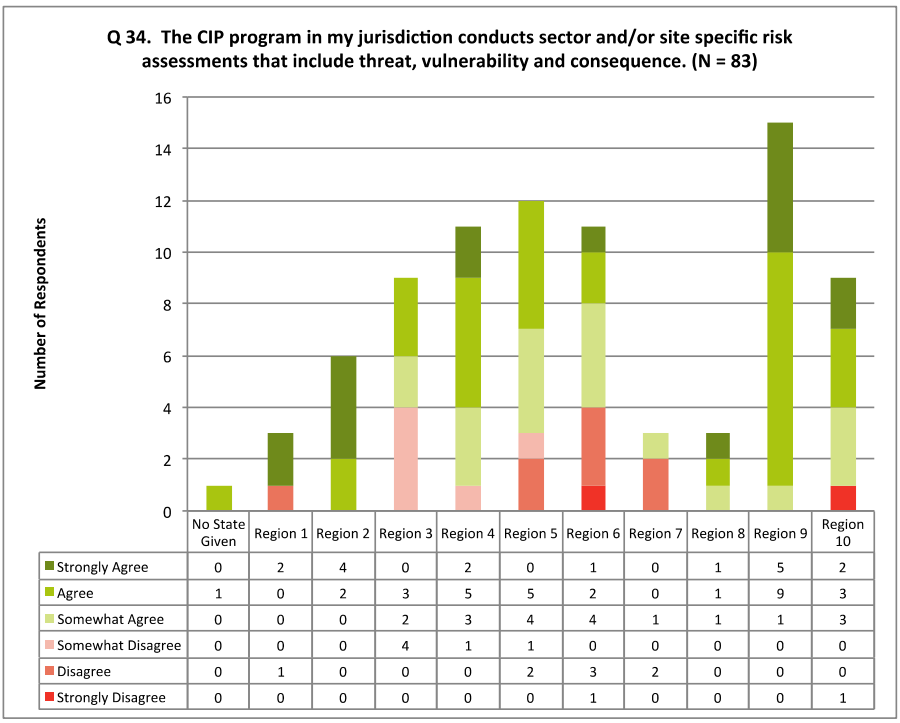
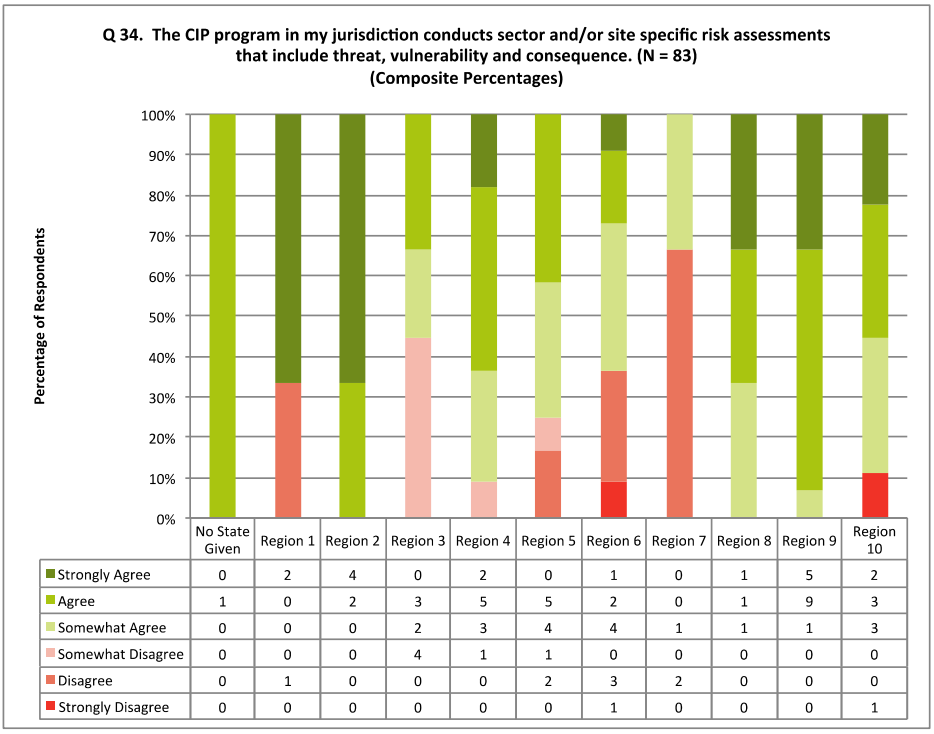


Figure 48B. Composite percentages of Figure 48A.



	No State Given	Region 1	Region 2	Region 3	Region 4	Region 5	Region 6	Region 7	Region 8	Region 9	Region 10
Strongly Agree	0	2	4	0	2	0	1	0	1	5	2
Agree	1	0	2	3	5	5	2	0	1	9	3
Somewhat Agree	0	0	0	2	3	4	4	1	1	1	3
Somewhat Disagree	0	0	0	4	1	1	0	0	0	0	0
Disagree	0	1	0	0	0	2	3	2	0	0	0
Strongly Disagree	0	0	0	0	0	0	1	0	0	0	1

Figure 48C. Figure 48 cross-analyzed by respondents federal FEMA region.



	No State Given	Region 1	Region 2	Region 3	Region 4	Region 5	Region 6	Region 7	Region 8	Region 9	Region 10
Strongly Agree	0	2	4	0	2	0	1	0	1	5	2
Agree	1	0	2	3	5	5	2	0	1	9	3
Somewhat Agree	0	0	0	2	3	4	4	1	1	1	3
Somewhat Disagree	0	0	0	4	1	1	0	0	0	0	0
Disagree	0	1	0	0	0	2	3	2	0	0	0
Strongly Disagree	0	0	0	0	0	0	1	0	0	0	1

Figure 48D. Composite percentages of Figure 48C.

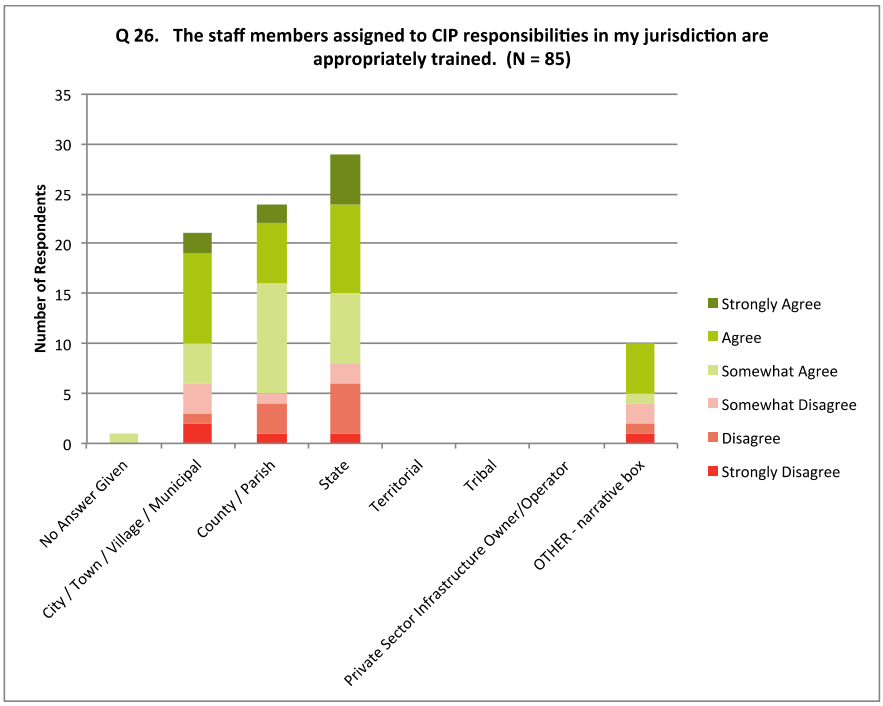


Figure 49A. Figure 49 cross-analyzed by respondents jurisdiction type.

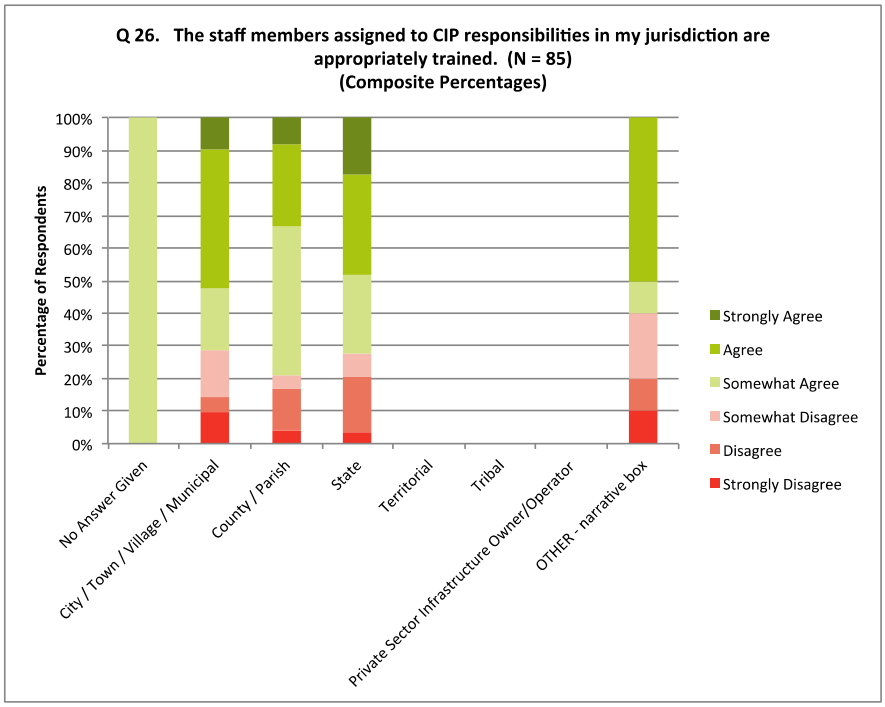
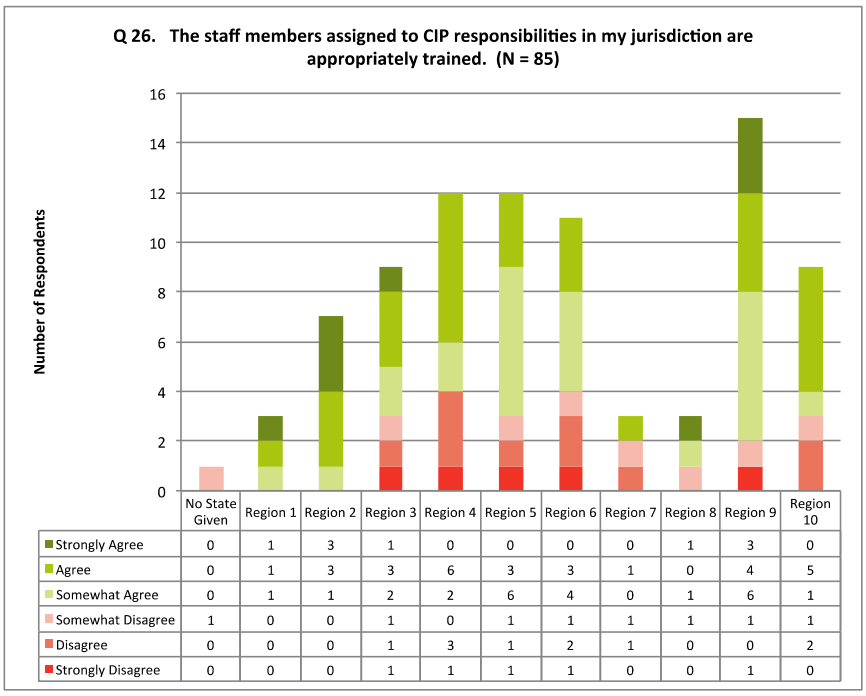
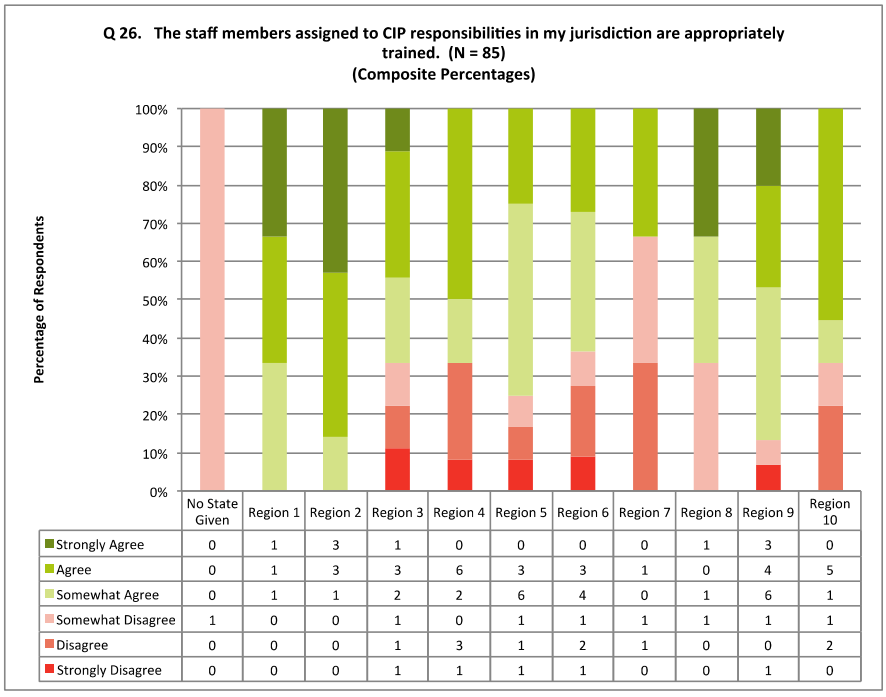


Figure 49B. Composite percentages of Figure 49A.



	No State Given	Region 1	Region 2	Region 3	Region 4	Region 5	Region 6	Region 7	Region 8	Region 9	Region 10
Strongly Agree	0	1	3	1	0	0	0	0	1	3	0
Agree	0	1	3	3	6	3	3	1	0	4	5
Somewhat Agree	0	1	1	2	2	6	4	0	1	6	1
Somewhat Disagree	1	0	0	1	0	1	1	1	1	1	1
Disagree	0	0	0	1	3	1	2	1	0	0	2
Strongly Disagree	0	0	0	1	1	1	1	0	0	1	0

Figure 49C. Figure 49 cross-analyzed by respondents federal FEMA region.



	No State Given	Region 1	Region 2	Region 3	Region 4	Region 5	Region 6	Region 7	Region 8	Region 9	Region 10
Strongly Agree	0	1	3	1	0	0	0	0	1	3	0
Agree	0	1	3	3	6	3	3	1	0	4	5
Somewhat Agree	0	1	1	2	2	6	4	0	1	6	1
Somewhat Disagree	1	0	0	1	0	1	1	1	1	1	1
Disagree	0	0	0	1	3	1	2	1	0	0	2
Strongly Disagree	0	0	0	1	1	1	1	0	0	1	0

Figure 49D. Composite percentages of Figure 49C.

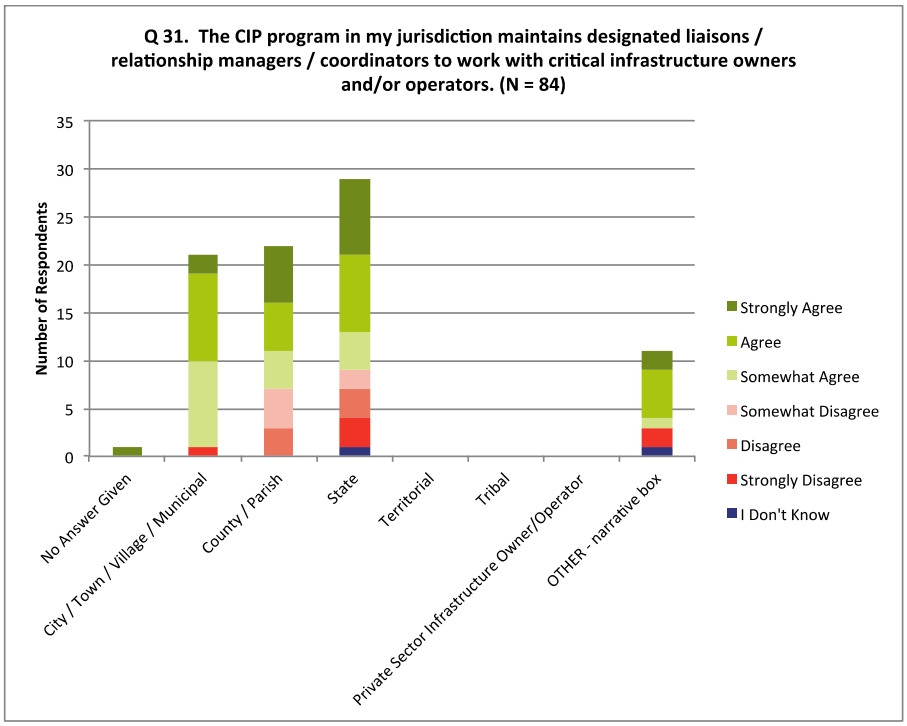


Figure 50A. Figure 50 cross-analyzed by respondents jurisdiction type.

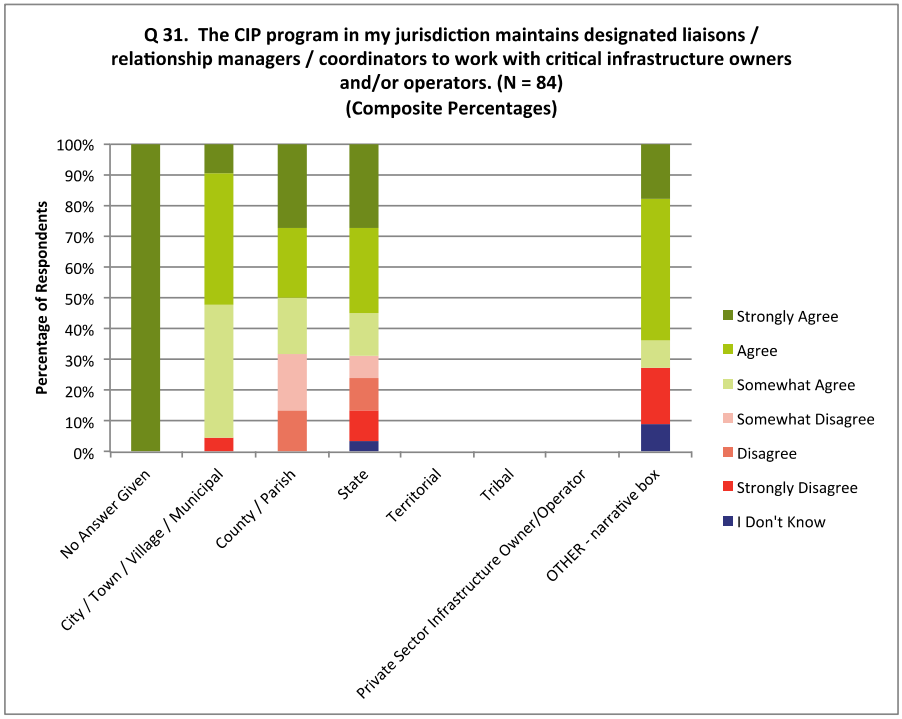
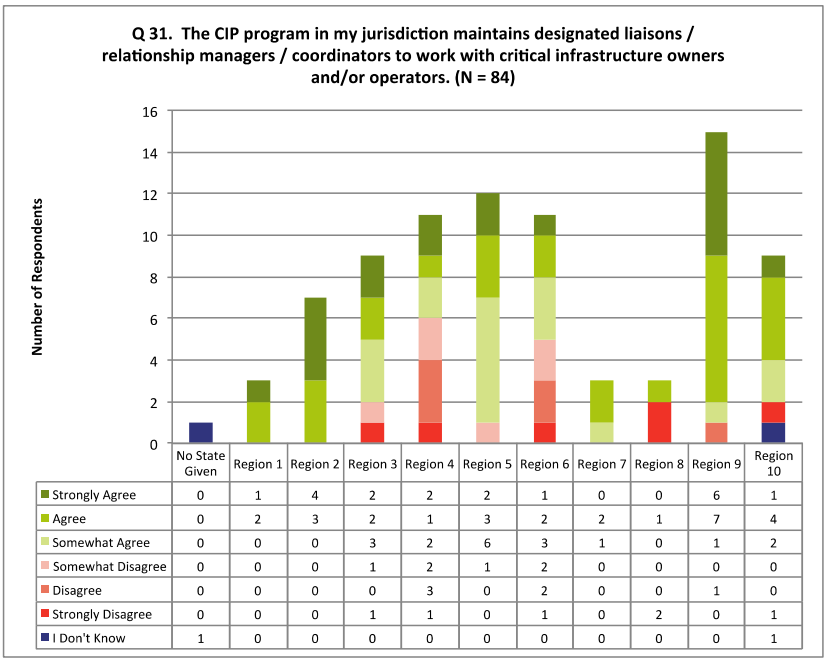
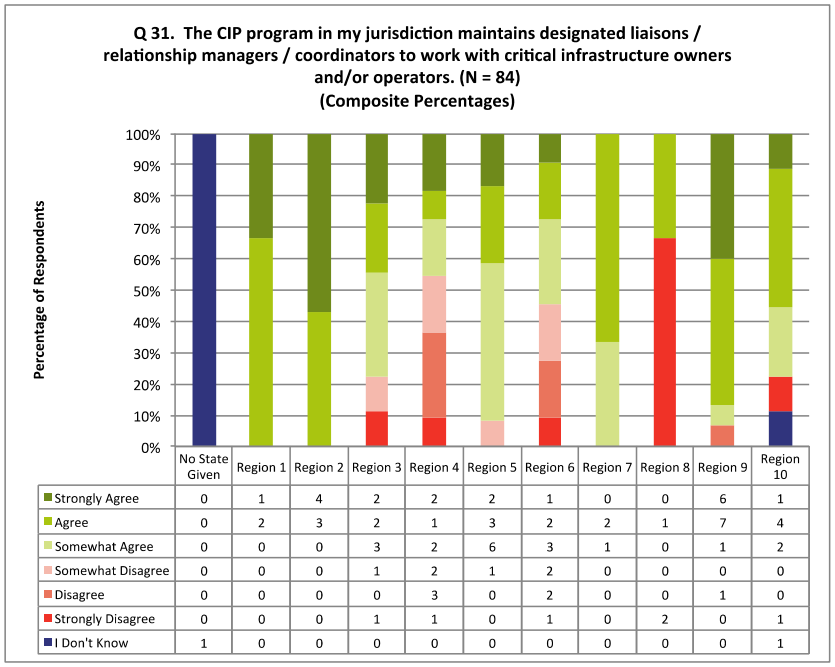


Figure 50B. Composite percentages of Figure 50A.



	No State Given	Region 1	Region 2	Region 3	Region 4	Region 5	Region 6	Region 7	Region 8	Region 9	Region 10
Strongly Agree	0	1	4	2	2	2	1	0	0	6	1
Agree	0	2	3	2	1	3	2	2	1	7	4
Somewhat Agree	0	0	0	3	2	6	3	1	0	1	2
Somewhat Disagree	0	0	0	1	2	1	2	0	0	0	0
Disagree	0	0	0	0	3	0	2	0	0	1	0
Strongly Disagree	0	0	0	1	1	0	1	0	2	0	1
I Don't Know	1	0	0	0	0	0	0	0	0	0	1

Figure 50C. Figure 50 cross-analyzed by respondents federal FEMA region.



	No State Given	Region 1	Region 2	Region 3	Region 4	Region 5	Region 6	Region 7	Region 8	Region 9	Region 10
Strongly Agree	0	1	4	2	2	2	1	0	0	6	1
Agree	0	2	3	2	1	3	2	2	1	7	4
Somewhat Agree	0	0	0	3	2	6	3	1	0	1	2
Somewhat Disagree	0	0	0	1	2	1	2	0	0	0	0
Disagree	0	0	0	0	3	0	2	0	0	1	0
Strongly Disagree	0	0	0	1	1	0	1	0	2	0	1
I Don't Know	1	0	0	0	0	0	0	0	0	0	1

Figure 50D. Composite percentages of Figure 50C.

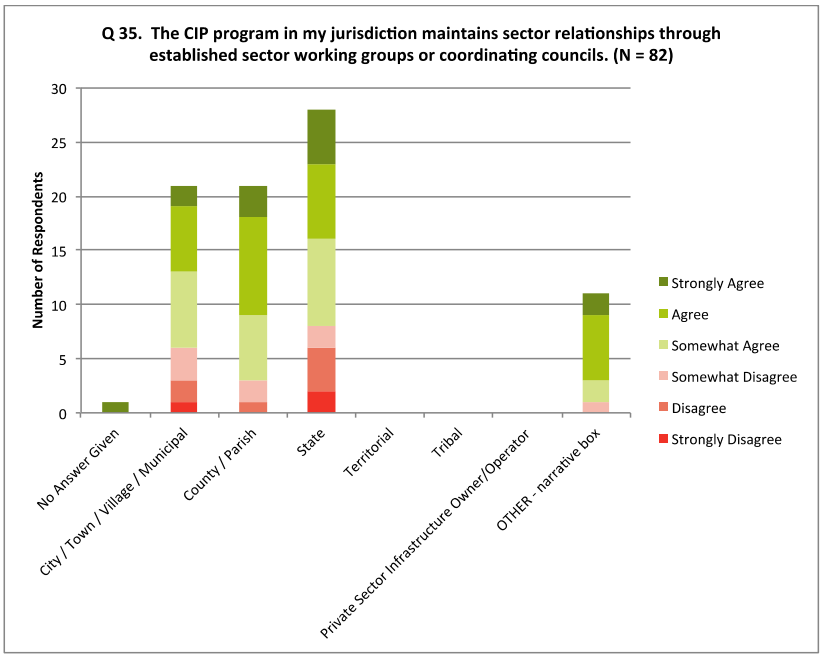


Figure 51A. Figure 51 cross-analyzed by respondents jurisdiction type.

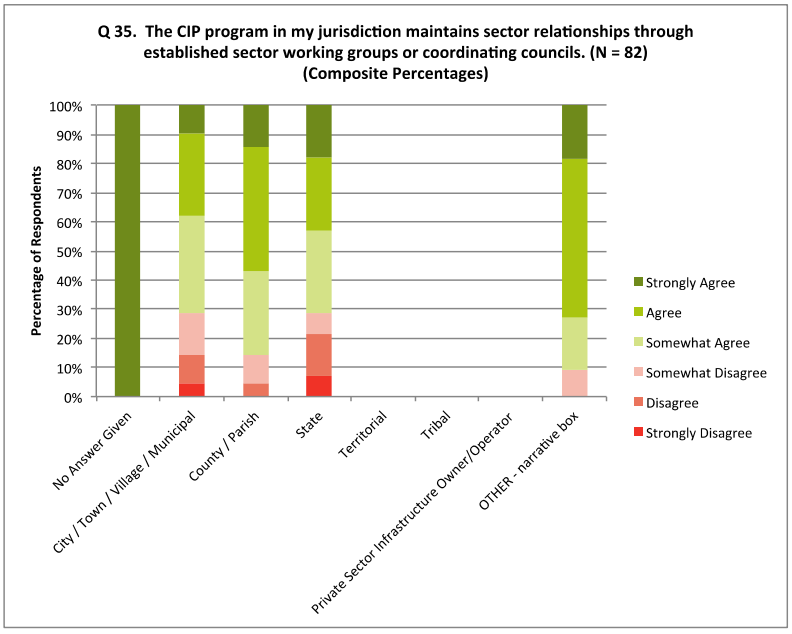
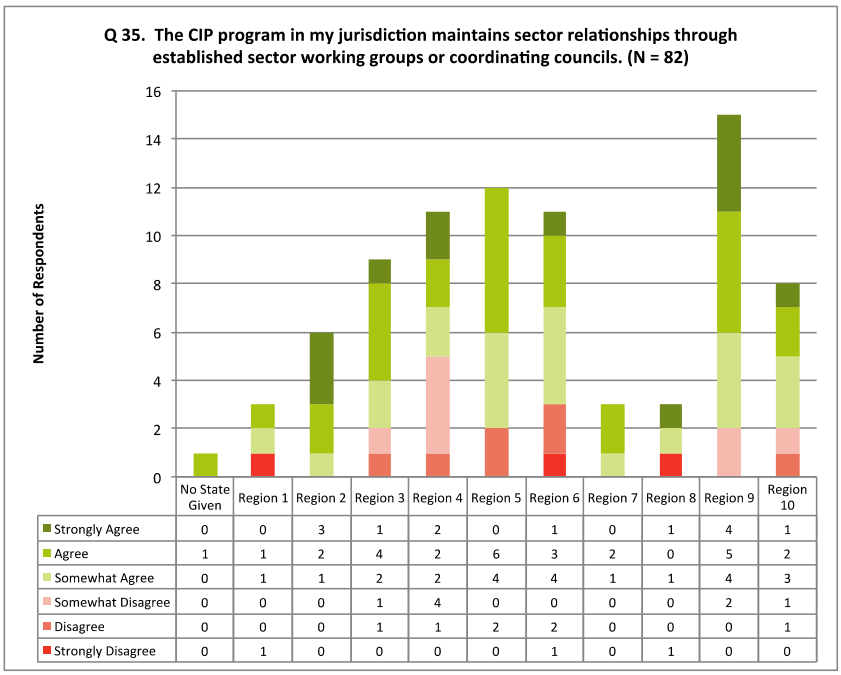
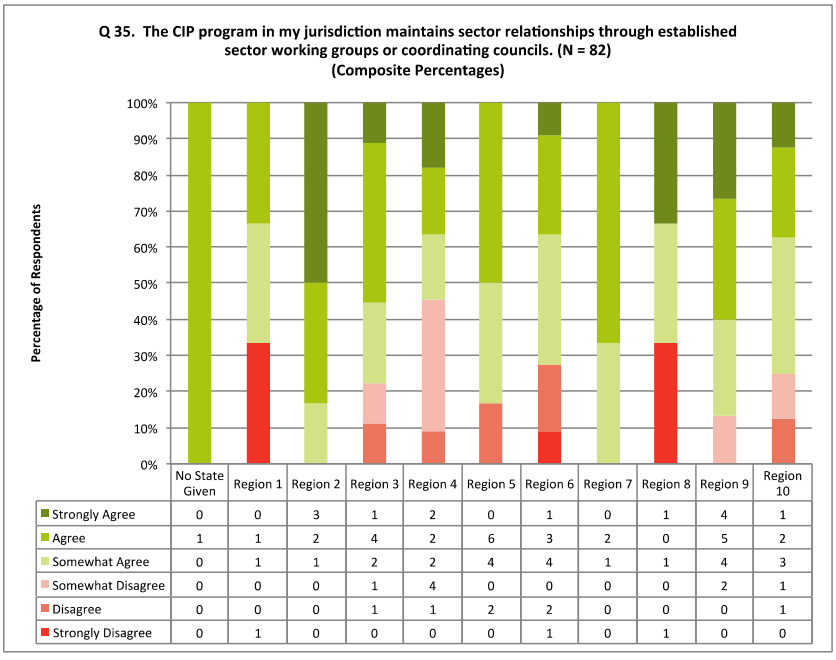


Figure 51B. Composite percentages of Figure 51A.



	No State Given	Region 1	Region 2	Region 3	Region 4	Region 5	Region 6	Region 7	Region 8	Region 9	Region 10
Strongly Agree	0	0	3	1	2	0	1	0	1	4	1
Agree	1	1	2	4	2	6	3	2	0	5	2
Somewhat Agree	0	1	1	2	2	4	4	1	1	4	3
Somewhat Disagree	0	0	0	1	4	0	0	0	0	2	1
Disagree	0	0	0	1	1	2	2	0	0	0	1
Strongly Disagree	0	1	0	0	0	0	1	0	1	0	0

Figure 51C. Figure 51 cross-analyzed by respondents federal FEMA region.



	No State Given	Region 1	Region 2	Region 3	Region 4	Region 5	Region 6	Region 7	Region 8	Region 9	Region 10
Strongly Agree	0	0	3	1	2	0	1	0	1	4	1
Agree	1	1	2	4	2	6	3	2	0	5	2
Somewhat Agree	0	1	1	2	2	4	4	1	1	4	3
Somewhat Disagree	0	0	0	1	4	0	0	0	0	2	1
Disagree	0	0	0	1	1	2	2	0	0	0	1
Strongly Disagree	0	1	0	0	0	0	1	0	1	0	0

Figure 51D. Composite percentages of Figure 43C.

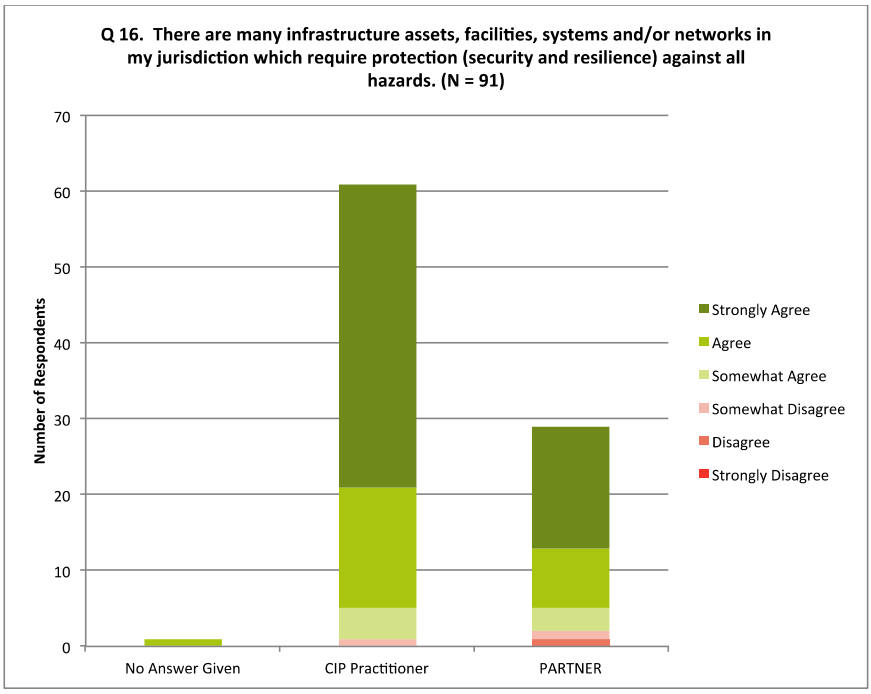


Figure 53A. Figure 53 cross-analyzed by respondents that self-identify as a CIP practitioner or partner.

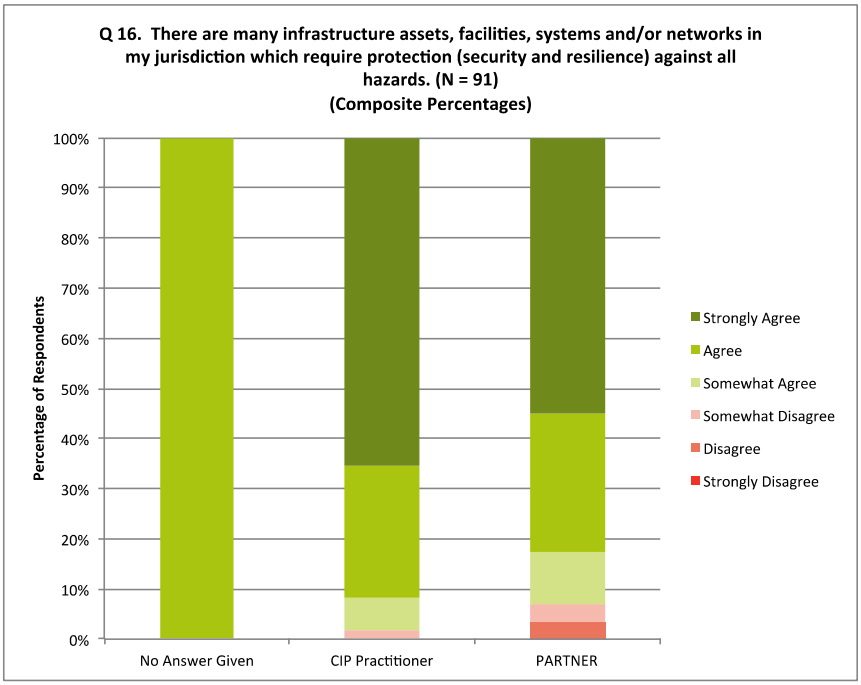


Figure 53B. Composite percentages of Figure 53A.

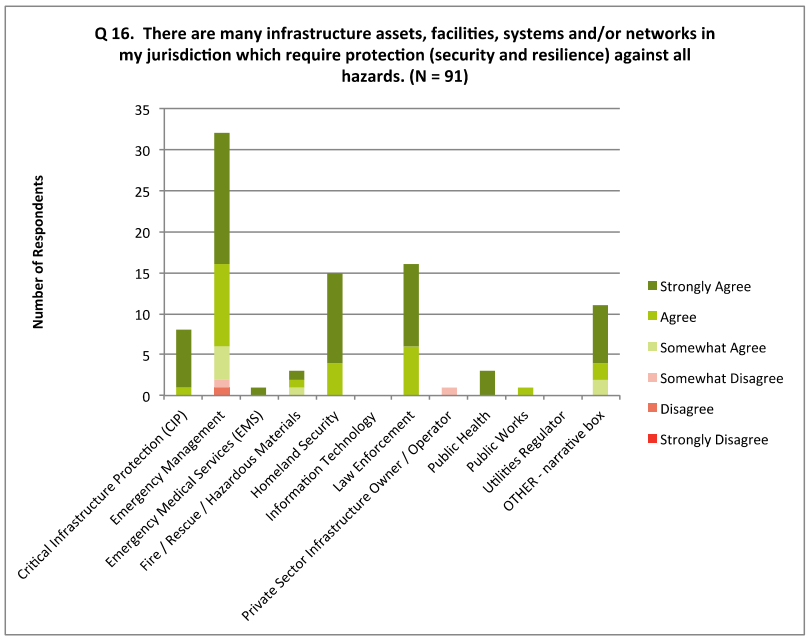


Figure 53C. Figure 53 cross-analyzed by respondents organization type.

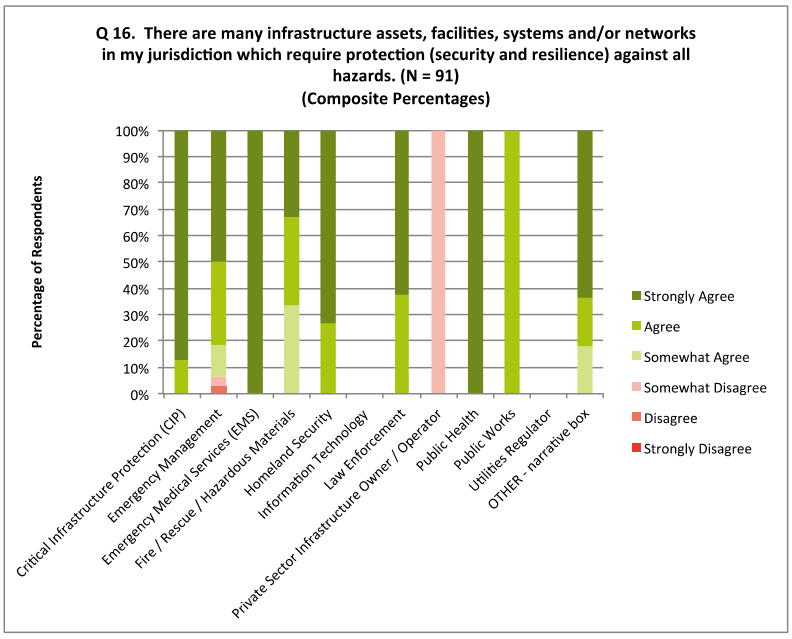


Figure 53D. Composite percentages of Figure 53C.

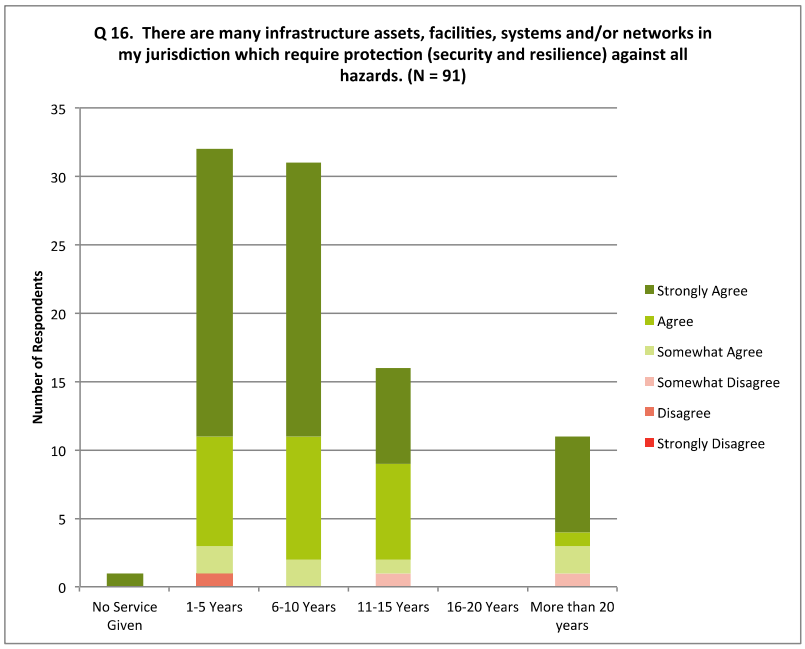


Figure 53E. Figure 53 cross-analyzed by respondents years of experience.

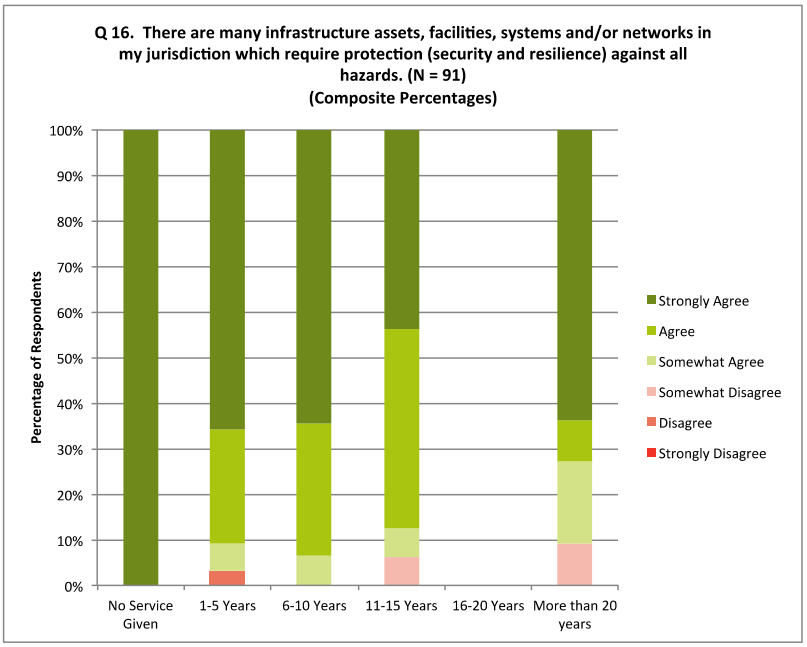


Figure 53F. Composite percentages of Figure 53E.

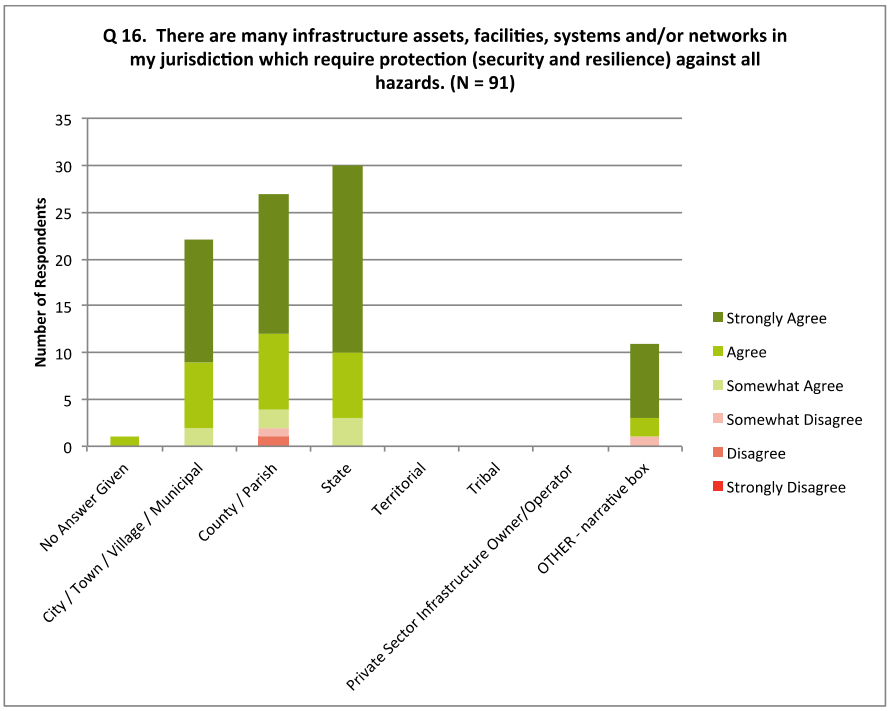


Figure 53G. Figure 53 cross-analyzed by respondents jurisdiction type.

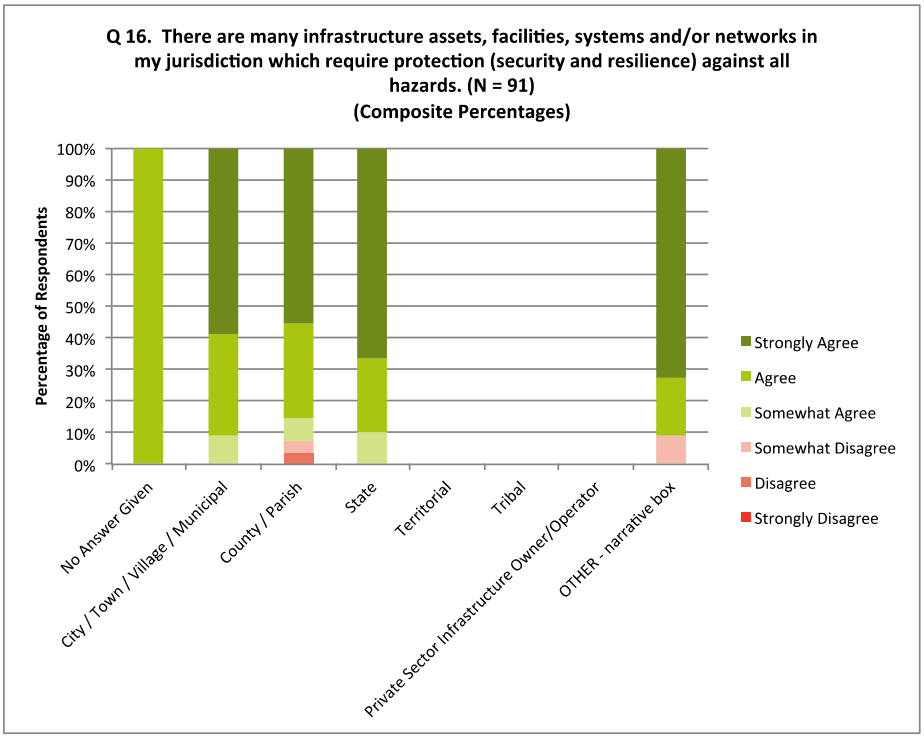
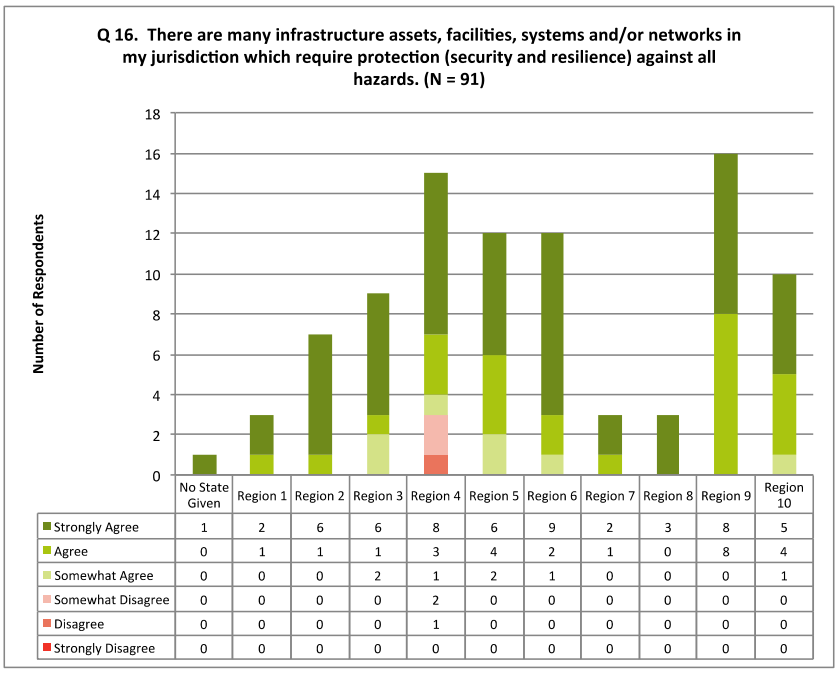
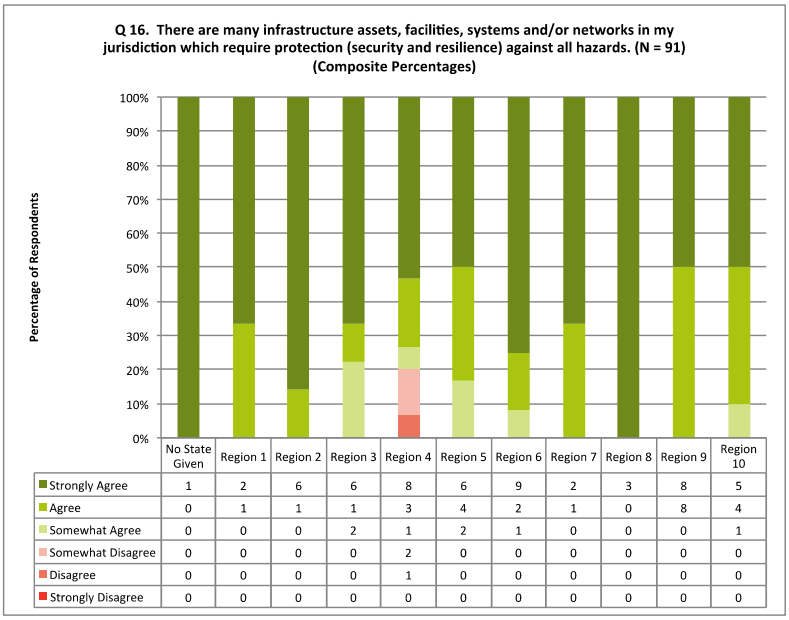


Figure 53H. Composite percentages of Figure 53G.



	No State Given	Region 1	Region 2	Region 3	Region 4	Region 5	Region 6	Region 7	Region 8	Region 9	Region 10
Strongly Agree	1	2	6	6	8	6	9	2	3	8	5
Agree	0	1	1	1	3	4	2	1	0	8	4
Somewhat Agree	0	0	0	2	1	2	1	0	0	0	1
Somewhat Disagree	0	0	0	0	2	0	0	0	0	0	0
Disagree	0	0	0	0	1	0	0	0	0	0	0
Strongly Disagree	0	0	0	0	0	0	0	0	0	0	0

Figure 53I. Figure 53 cross-analyzed by respondents federal FEMA region.



	No State Given	Region 1	Region 2	Region 3	Region 4	Region 5	Region 6	Region 7	Region 8	Region 9	Region 10
Strongly Agree	1	2	6	6	8	6	9	2	3	8	5
Agree	0	1	1	1	3	4	2	1	0	8	4
Somewhat Agree	0	0	0	2	1	2	1	0	0	0	1
Somewhat Disagree	0	0	0	0	2	0	0	0	0	0	0
Disagree	0	0	0	0	1	0	0	0	0	0	0
Strongly Disagree	0	0	0	0	0	0	0	0	0	0	0

Figure 53J. Composite percentages of Figure 53I.

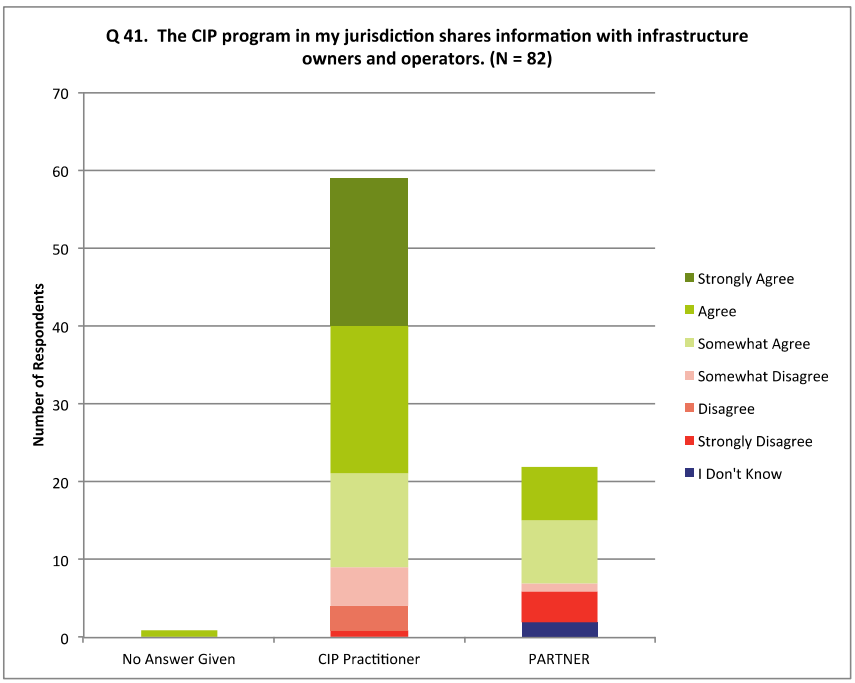


Figure 56A. Figure 56 cross-analyzed by respondents that self-identify as a CIP practitioner or partner.

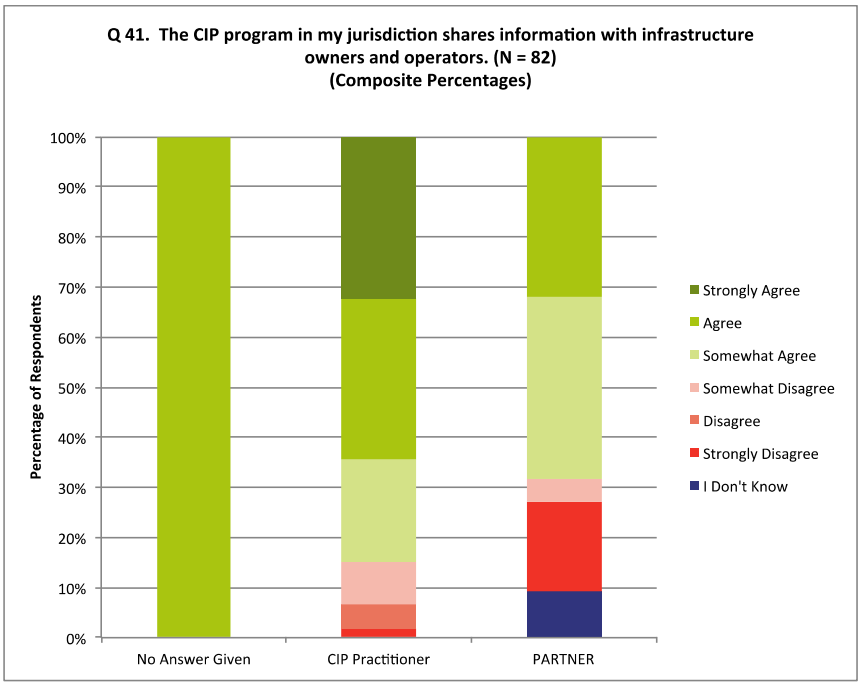


Figure 56B. Composite percentages of Figure 56A.

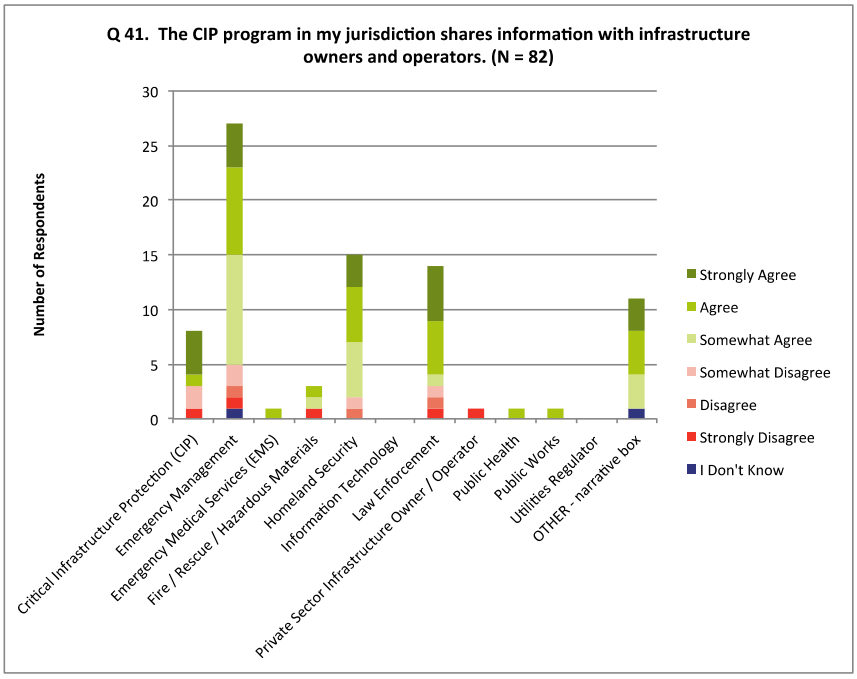


Figure 56C. Figure 56 cross-analyzed by respondents organization type.

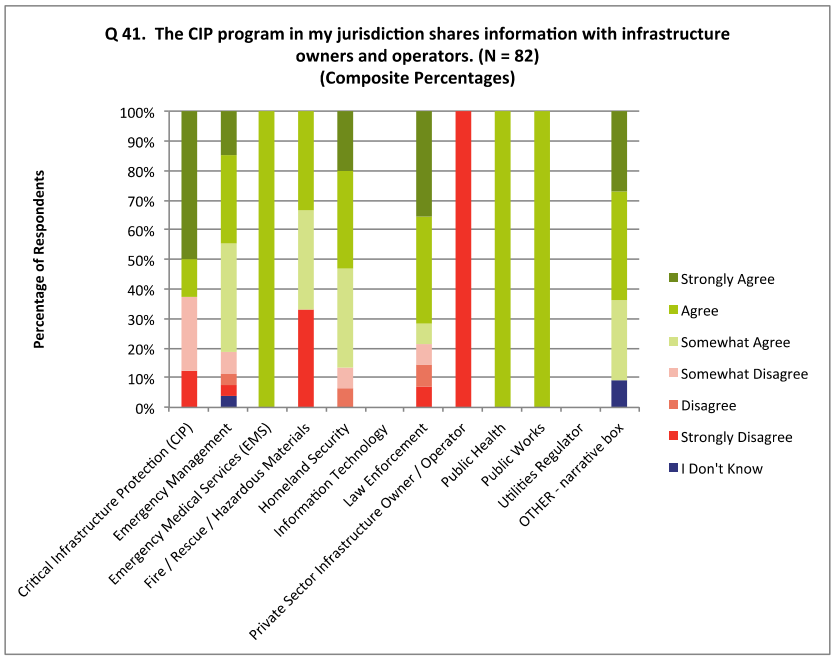


Figure 56D. Composite percentages of Figure 56C.

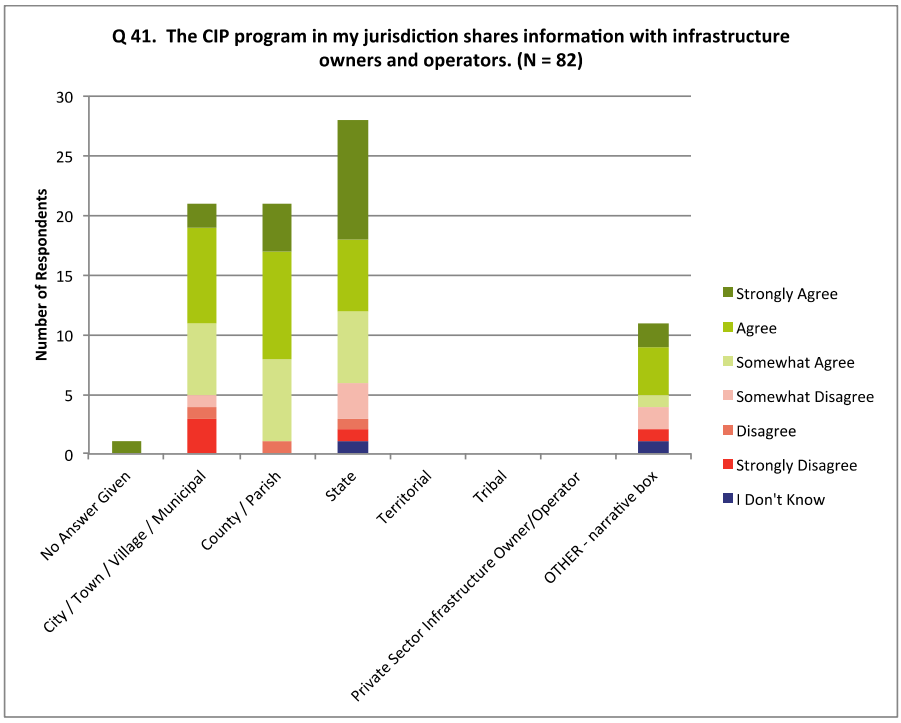


Figure 56E. Figure 56 cross-analyzed by respondents jurisdiction type.

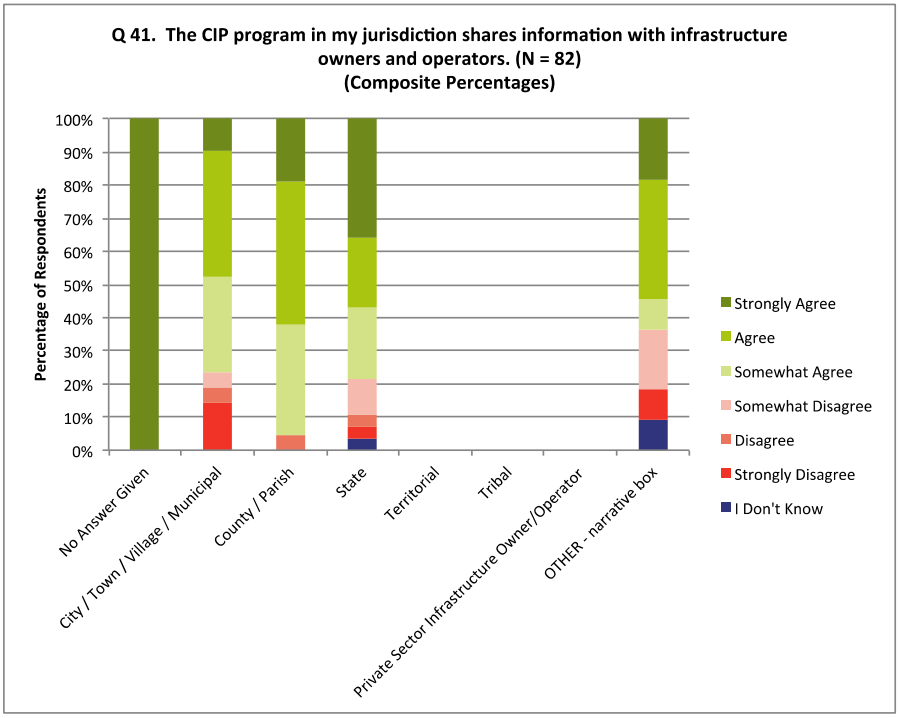


Figure 56F. Composite percentages of Figure 56E.

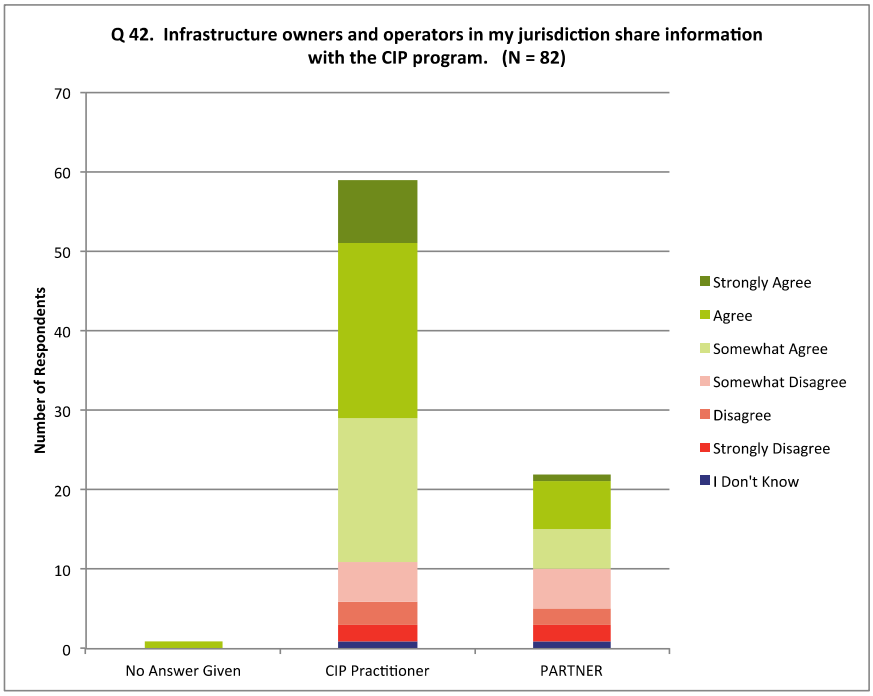


Figure 57A. Figure 57 cross-analyzed by respondents that self-identify as a CIP practitioner or partner.

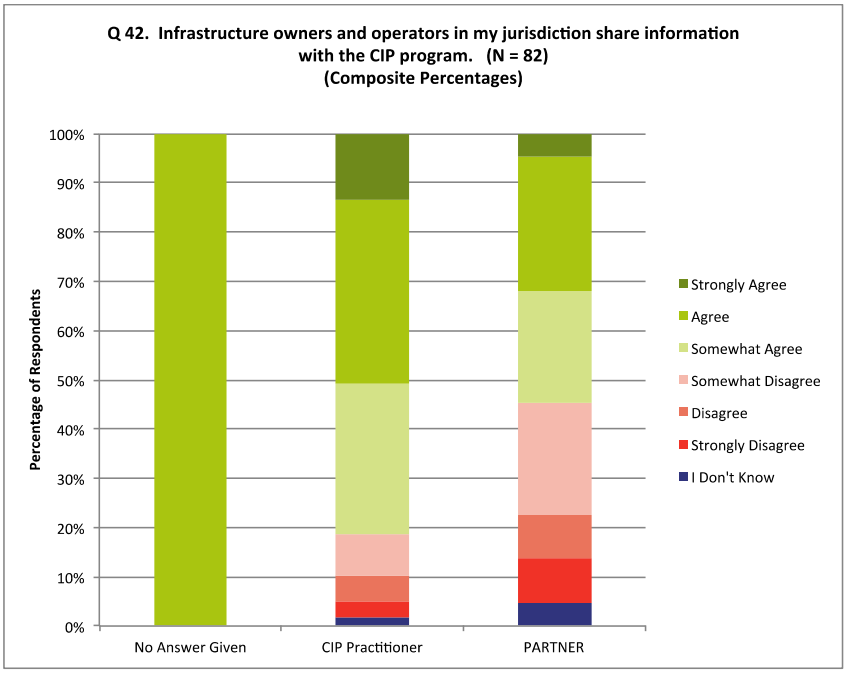


Figure 57B. Composite percentages of Figure 57A.

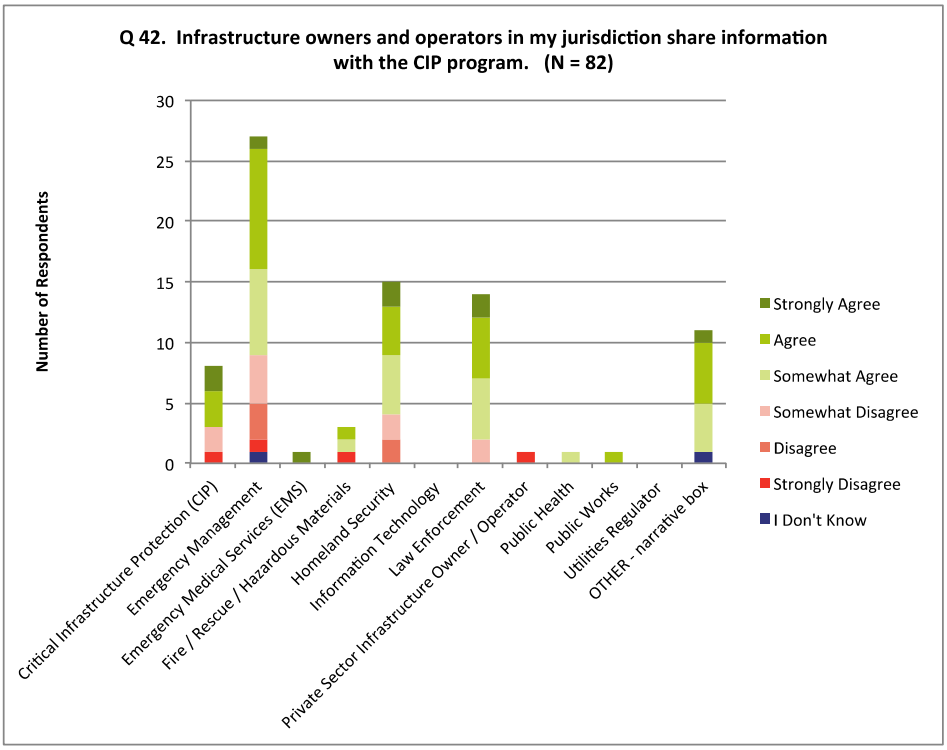


Figure 57C. Figure 57 cross-analyzed by respondents organization type.

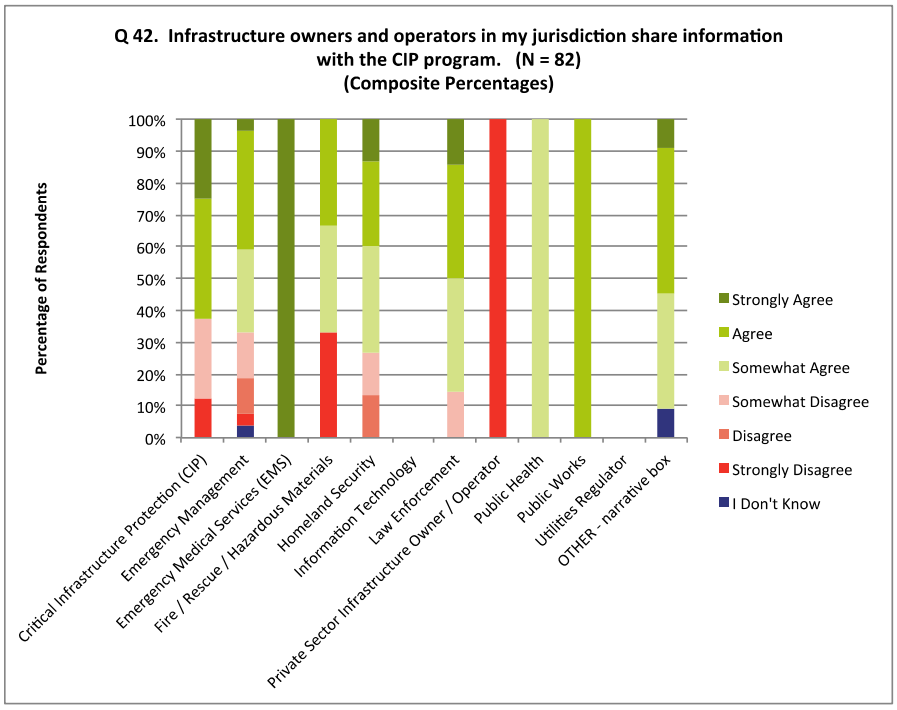


Figure 57D. Composite percentages of Figure 57C.

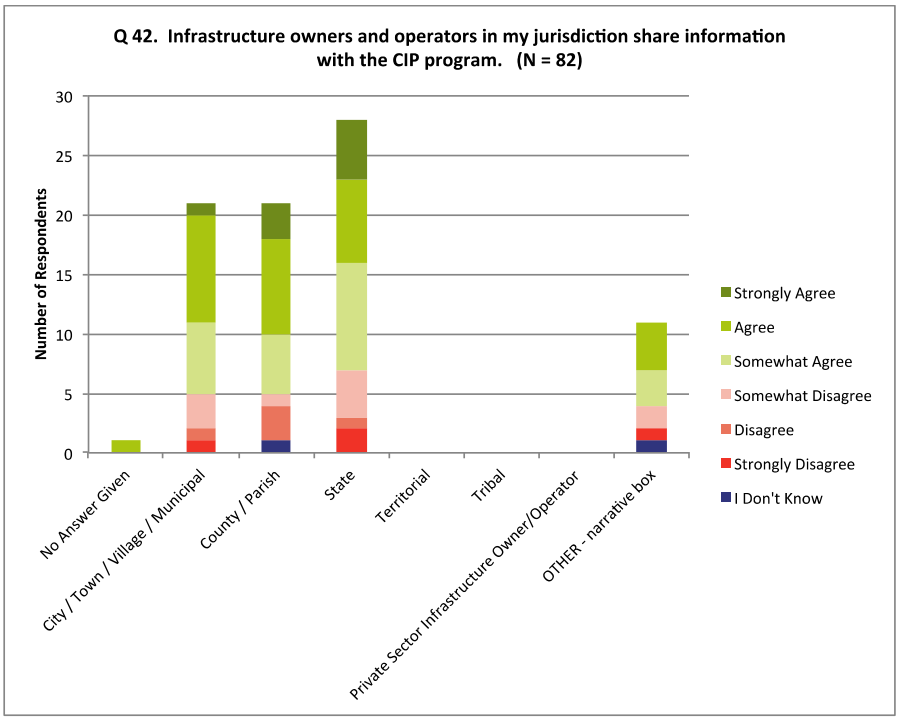


Figure 57E. Figure 57 cross-analyzed by respondents jurisdiction type.

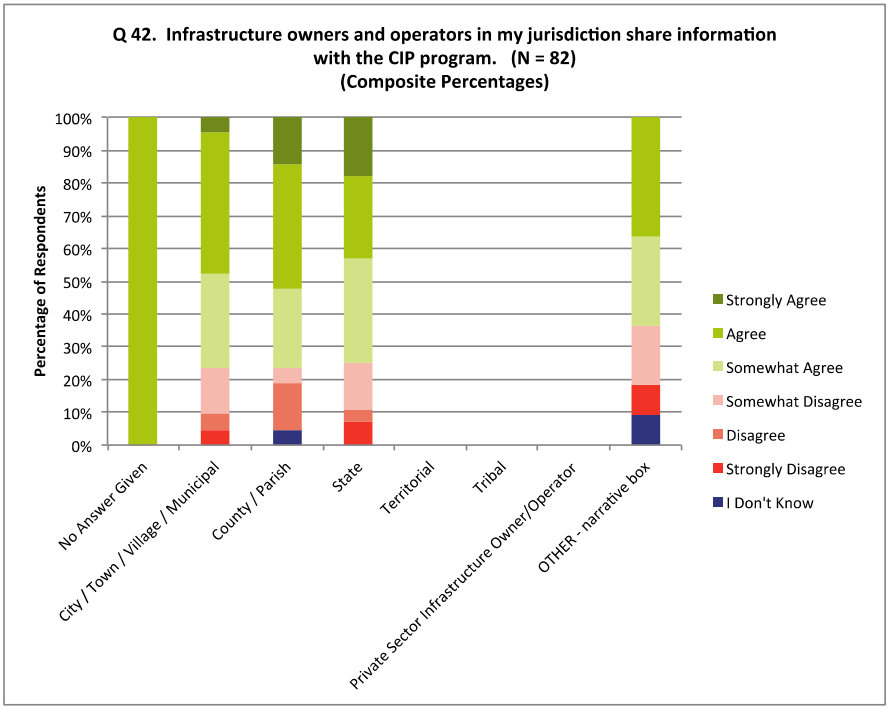


Figure 57F. Composite percentages of Figure 57E.

APPENDIX D. NARRATIVE RESPONSE TABLES

TABLE 6: Question 4—My organization is best described as one of the following: NARRATIVE RESPONSES *Entries appear exactly as submitted by respondents*
State of NM Homeland Security and Emergency Management
Multidisciplinary
UASI administered by Law Enforcement
Note: My organization is the Texas Department of Public Safety, which is the lead State Law Enforcement Agency for Texas. However, my division within the agency is the Texas Joint Crime Information Center (Fusion Center). It should also be noted that my position requires more interaction with the Emergency Management Division than other functions in the fusion center.
Public Sector Infrastructure owner / Operator (State Government)
Community Owned Four Service Utility: Electric, Natural Gas, Water, Wastewater
State Government—Florida Department of Transportation
Esf-8 health and medical
My organization is responsible for the State and UASI Fusion Centers, State Emergency management and Homeland Security.
State Cabinet Secretariat overseeing all public safety state agencies and homeland security functions, with the Cabinet Secretary serving as the Homeland Security Advisor.
National Domestic Preparedness.
Law Enforcement Officer assigned to the local fusion center CIP unit
Specifically I focus on Critical Infrastructure Protection
Homeland Security—Employed by EMA and have a seat in the state EOC, head up the CIP effort in the state while working out of the state's designated fusion center.
The agency has Emergency Management and Homeland Security responsibilities, which CIP comes under.
Emergency Management and Homeland Security
Missouri Office of Homeland Security serving as the Critical Infrastructure Program Manager.

TABLE 7: Question 5—Please choose one of the following that best describes your role within your organization: NARRATIVE RESPONSES *Entries appear exactly as submitted by respondents*
Critical infrastructure coordinator
Analyst assigned to CIKR
Analyst
Strategic Planner and author of the Texas Infrastructure Security and Resiliency Plan.
Infrastructure Protection Specialist
EM/HS Coordinator
Analyst
Planner
Chief of Staff
Lead Planner/Analyst
Protective Security Advisor
Emergency Services Coordinator
Company Security Officer / Emergency Management Coordinator.
Emergency Manager
owner
Emergency Coordination Officer.
Logistics section chief
Liaison/Subject Matter Expert/Advisor
Analyst
Grant Coordinator
Chairman of the NDPC
My boss is the supervisor/team leader
Current Title is: GIS / CIKR Planning Section Chief

TABLE 8: Question 7—My jurisdiction is: NARRATIVE RESPONSES *Entries appear exactly as submitted by respondents*
fusion center
Airport/Marine
Regional
multi county
Urban area encompassing an eight county region
Federal
97 West Texas Counties
Washington State Ferries operates our to 8 counties. We also operate on international route to Sidney B.C.
USA
National Capital Region (MD/DC/VA)
District of Columbia
National

TABLE 9: Question 36——The CIP program in my jurisdiction maintains an engagement model with infrastructure owners and operators DIFFERENT from sector working groups or coordinating councils——IF YES, please describe in the narrative box provided. NARRATIVE RESPONSES *Entries appear exactly as submitted by respondents*
I have frequent engagement (threat briefings, site assessments) with private sector partners and local utilities and associations such as the AWRA and AWWA.
Oil and Gas Industry—regulatory oversight
We maintain a relationship with private sector representatives through the Private Sector Advisory Council (all sectors represented through trade organizations). We maintain a relationship with public sector partners through the Homeland Security Council to ensure the actions of State Government are coordinated.
The CIP will reach out to private critical infrastructure
Regional Emergency Management meetings
Our organization has its own Alternative Security Plan (ASP) Approved Security Plan approved by USCG.
Participation in regional emergency management; and, security threat working groups. Also close relationship with FBI and local PD.
Attend ECIP Visits and assessments with local PSA, recurring security working group meetings
Direct coordination and contact with public/private sector partners. We did have a national best practice council at one time, but this was neglected and ultimately became non-operational.
Via. the New Mexico Office of Homeland Security
NYs organization of this is varied by sector and geography; additionally meetings and events are hosted on an as needed basis and include regulatory partners and state agencies and authorities that have natural relationships with the specific infrastructure sector or industry.
As part of our local Planning Exercise and Training (PET) region, we have a CI/KR working group comprised mainly of private sector entities
CIP program staff equals one. I have qualified people in both the EMA, MSP and fusion center that I often utilize for specific tasks / assessments. I answered YES because my engagement with GCC's and working groups is a decision I make after considering the time commitment and benefits.
Statewide Infrastructure Protection Sub-Committee with representation from both public and private sector across identified sectors, in addition to an alliance with the Pacific Northwest Economic Region (PNWER)
SME contacts have been developed through the years and I am on the board of the FBI InfraGard program, which assists in engaging owners/operators as needed.
Rely heavily on county\local partners to engage CIKR owners through training and seats in their EOCs during response. We assist where we can to facilitate those relationships and gather site information through ACAMS. Loss of access to ACAMS and absence of an alternative has put our "State" program on hold. But the relationships at the local\county levels endure.

APPENDIX E. QUESTION "N" AND AVERAGE TABLE

TABLE 10: Total responses (N) and averages by survey question number

Survey Question Number	Total Responses (N)	Averages
1	91	not applicable
2	90	not applicable
3	90	not applicable
4	91	not applicable
5	91	not applicable
6	90	9.07
7	91	not applicable
8	87	3.63
9	90	4.18
10	91	4.91
11	91	3.62
12	90	4.92
13	91	not applicable
14	91	4.93
15	91	3.52
16	91	5.46
17	89	not applicable
18	85	0.43
19	88	not applicable
20	86	4.69
21	85	not applicable
22	47	4.87
23	85	not applicable
24	24	4.25
25	86	2.62
26	85	4.05
27	51	not applicable
28	38	not applicable
29	85	2.95
30	84	3.93
31	84	4.25
32	84	not applicable
33	83	4.39
34	83	4.45
35	82	4.28
36	82	not applicable
37	81	4.14
38	83	3.61
39	82	3.59

Survey Question Number	Total Responses (N)	Averages
40	82	3.57
41	82	4.37
42	82	4.09
43	83	3.12
44	83	3.55
45	83	3.64
46	83	3.47
47	81	4.00
48	52	not applicable

LIST OF REFERENCES

Broughton, Pamela N. “Measuring Preparedness: Assessing the Impact of the Homeland Security Grant Program.” Master’s thesis, Naval Postgraduate School, 2009.

Carlson, L., G. Bassett, W. Buehring, M. Collins, S. Folga, B. Haffenden, F. Petit, J. Phillips, D. Verner, and R. Whitfield. *Resilience: Theory and Applications*. Argonne, IL: Argonne National Laboratory: Decision and Information Sciences Division, 2012. http://www.ipd.anl.gov/anlpubs/2012/02/72218.pdf.

Committee on Increasing National Resilience to Hazards and Disasters. *Disaster Resilience: A National Imperative*. Washington, DC: National Academies Press, 2012. http://resilience.abag.ca.gov/wp-content/documents/resilience/toolkit/Disaster%20Resilience_A%20National%20Imperative.pdf.

Commonwealth of Australia. *Critical Infrastructure Resilience Strategy*. 2010. http://www.ag.gov.au/Nationalsecurityandcounterterrorism/Pages/CriticalInfrastructureResilience.aspx.

———. *Critical Infrastructure Resilience Strategy Supplement: An Overview of Activities to Deliver the Strategy*. 2010. http://www.emergency.qld.gov.au/publications/pdf/Critical_Infrastructure_Resilience_Strategy_Supplement.pdf.

Council of Australian Governments, *National Strategy for Disaster Resilience*. Barton, Australia: Council of Australian Governments, 2011. https://www.ag.gov.au/EmergencyManagement/Documents/NationalStrategyforDisasterResilience.pdf.

Egli, Dane S. *Beyond the Storms: Strengthening Homeland Security and Disaster Management to Achieve Resilience*. 1st ed. Armonk, NY: M. E. Sharpe, Inc., 2014.

Else, Daniel H. *Defense Production Act: Purpose and Scope* (RS20587). Washington, DC: Congressional Research Service, 2008. http://fas.org/sgp/crs/natsec/RS20587.pdf.

Federal Emergency Management Agency. *Crisis Response and Disaster Resilience 2030: Forging Strategic Action in an Age of Uncertainty: Progress Report Highlighting the 2010-2011 Insights of the Strategic Foresight Initiative*. Washington, DC: Federal Emergency Management Agency, 2012.

———. *Fiscal Year 2010 Buffer Zone Protection Program: Guidance and Application Kit*. Washington, DC: Federal Emergency Management Agency, 2012. http://www.fema.gov/media-library-data/20130726-1750-25045-6174/fy_2010_bzpp_guidance_final.pdf.

———. *Fiscal Year 2014 Homeland Security Grant Program Supplemental Resource*. Washington, DC: Federal Emergency Management Agency, 2014. http://www.fema.gov/media-library-data/1395243947274-507831e9fb40d412030789b609a555bc/FY%202014%20Supplemental%20Guidance_Regional%20Resiliency%20Assessment%20Program_Final.pdf.

———. *Funding Opportunity Announcement: FY 2014 Emergency Management Performance Grant*. Washington, DC: Federal Emergency Management Agency, 2014. http://www.fema.gov/media-library-data/1398433298042-f8d5c17604fdb97c5ef5b49419a7cf01/FY2014_EMPG_FOA_Revised_508.pdf.

———. *Funding Opportunity Announcement (FOA) FY 2014 Homeland Security Grant Program (HSGP)*. Washington, DC: Federal Emergency Management Agency, 2014. http://www.fema.gov/media-library-data/1395161200285-5b07ed0456056217175fbdee28d2b06e/FY_2014_HSGP_FOA_Final.pdf.

———. *U.S. Department of Homeland Security Funding Opportunity Announcement (FOA) FY 2014 Port Security Grant Program (PSGP)*. Washington, DC: Federal Emergency Management Agency, 2014. http://www.fema.gov/media-library-data/1396623742630-9e497a99bef3e3c0265bbf84993b5e69/FY_2014_PSGP_FOA_Final_Revised.pdf.

Fisher, R. E., G. W. Bassett, W. A. Buehring, M. J. Collins, D. C. Dickinson, L. K. Eaton, K. E. Wallace, R. G. Whitfield, and J. P. Peerenboom. *Constructing a Resilience Index for the Enhanced Critical Infrastructure Protection Program*. Argonne, IL: Argonne National Laboratory: Decision and Information Sciences Division, August 2010. http://www.ipd.anl.gov/anlpubs/2010/09/67823.pdf.

Hardenbrook, Brandon J. “The Need for a Policy Framework to Develop Disaster Resilient Regions.” *Journal of Homeland Security and Emergency Management* 2, no. 3 (2005): 1–23. doi:10.2202/1547-7355.1133.

Lau, Constance H. and Beverly Scott. “Strengthening Regional Resilience through National, Regional and Sector Partnerships—DRAFT Report and Recommendations.” Washington, DC: National Infrastructure Advisory Council, 2013. http://www.dhs.gov/sites/default/files/publications/niac-rrwg-report-final-review-draft-for-qbm.pdf.

Linacre, John M. “Investigating Rating Scale Category Utility.” *Journal of Outcome Measurement: Dedicated to Health, Education and Social Science* 3, no. 2 (1999): 103–122.

Parsons, Curtis, and Brian Wright. *Summary of Regional Reports: Critical Infrastructure Programs 2011–2013*. Washington, DC: United States Department of Homeland Security: State, Local, Tribal, and Territorial Government Coordinating Council.

Lewis, Ted G. *Bak’s Sand Pile: Strategies for a Catastrophic World*. Williams, CA: Agile Press, 2011.

National Infrastructure Advisory Council. *Critical Infrastructure Resilience: Final Report and Recommendations*. Washington, DC: National Infrastructure Advisory Council, 2009. http://www.dhs.gov/xlibrary/assets/niac/niac_critical_infrastructure_resilience.pdf.

Petit, F. D., G. W. Bassett, R. Black, W. A. Buehring, M. J. Collins, D. C. Dickinson, R. E. Fisher, et al. *Resilience Measurement Index: An Indicator of Critical Infrastructure Resilience*. Argonne, IL: Argonne National Laboratory: Decision and Information Sciences Division, 2013. http://www.ipd.anl.gov/anlpubs/2013/07/76797.pdf.

Pritzker, Penny. “Community Resilience Planning Guide for Buildings and Infrastructure Systems: Volume I: Draft for Public Comment.” Washington, DC: National Institute of Standards and Technology, 2015. http://www.nist.gov/el/building_materials/resilience/upload/NIST_Guide_Volume_1_042515_For-Web-2.pdf.

———. “Community Resilience Planning Guide for Buildings and Infrastructure Systems: Volume II: Draft for Public Comment.” Washington, DC: National Institute of Standards and Technology, 2015. http://www.nist.gov/el/building_materials/resilience/upload/NIST_Guide_Volume_2_042515_For-Web-2.pdf.

Puleo, Stephen. *Dark Tide: The Great Boston Molasses Flood of 1919*. Boston, MA: Beacon Press, 2004.

Rattray, Janice, and Martyn C Jones. “Issues in Clinical Nursing: Essential Elements of Questionnaire Design and Development.” *Journal of Clinical Nursing* 16 (2005): 234–243. doi:10.1111/j.1365-2702.2006.01573.x.

Sagarin, Raphael. “Natural Security for a Variable and Risk-Filled World.” *Homeland Security Affairs* 6, no. 3 (2010): 1–20. https://www.hsaj.org/articles/79.

U.S. Government Accountability Office. *Homeland Security: Effective Regional Coordination Can Enhance Emergency Preparedness* (GAO-04-1009). Washington, DC: U.S. Government Accountability Office, 2004. http://www.gao.gov/assets/250/244172.pdf.

U.S. Department of Homeland Security. *Homeland Security Presidential Directive 7: Critical Infrastructure Identification, Prioritization, and Protection*. Washington, DC: U.S. Department of Homeland Security, 2003. http://www.dhs.gov/homeland-security-presidential-directive-7.

———. *National Infrastructure Protection Plan: Partnering to Enhance Protection and Resiliency*. U.S. Department of Homeland Security, 2009.

———. *National Prevention Framework*. Washington, DC: U.S. Department of Homeland Security, 2013. http://www.fema.gov/media-library-data/20130726-1913-25045-6071/final_national_prevention_framework_20130501.pdf.

———. *National Protection Framework*, 1st ed. Washington, DC: U.S. Department of Homeland Security, 2014. http://www.fema.gov/media-library-data/1406717583765-996837bf788e20e977eb5079f4174240/FINAL_National_Protection_Framework_20140729.pdf.

———. *NIPP 2013: Partnering for Critical Infrastructure Security and Resilience*. Washington, DC: U.S. Department of Homeland Security, 2013. http://www.dhs.gov/publication/nipp-2013-partnering-critical-infrastructure-security-and-resilience.

———. *NIPP Supplemental Tool: Connecting to the NICC and NCCIC*. Washington, DC: U.S. Department of Homeland Security, 2013. http://www.dhs.gov/sites/default/files/publications/NIPP-2013-Supplement-Connecting-to-the-NICC-and-NCCIC-508.pdf.

U.S. Department of Justice. *Regional Information Sharing Systems (RISS) Program* [brochure]. Washington, DC: U.S. Department of Justice, 2014. Accessed December 5, 2014. https://www.riss.net/default/Overview.

White House. *The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets*. Washington, DC: White House, 2003.

———. *Presidential Policy Directive/PPD-21: Critical Infrastructure Security and Resilience*. Washington, DC: White House, 2013. https://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil.

Wiggins, Chanl. *Use of the Defense Production Act to Reduce Interruptions in Critical Infrastructure and Key Resource Operations during Emergencies: Fiscal Year 2009 Report to Congress*. Washington, DC: Federal Emergency Management Agency, 2009.

Zolli, Andrew. *Resilience: Why Things Bounce Back*, 1st ed. New York: Free Press, 2012.

THIS PAGE INTENTIONALLY LEFT BLANK

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California